PRACE NAUKOWE UNIWERSYTETU EKONOMICZNEGO WE WROCŁAWIU nr 55
Informatyka Ekonomiczna 13 2009

Jakub Krasicki
Uniwersytet Ekonomiczny we Wrocławiu

ZARZĄDZANIE BEZPIECZEŃSTWEM SYSTEMU INFORMACYJNEGO W ŚWIETLE MIĘDZYNARODOWYCH STANDARDÓW ISO/IEC 17799 ORAZ ISO/IEC 13335

Streszczenie: Wpływ nowych technologii na bezpieczeństwo systemów informacyjnych jest bardzo duży. Z tego względu musimy utrzymywać bezpieczeństwo tych systemów na odpowiednim poziomie. W artykule najpierw zdefiniowano pojęcia bezpieczeństwa systemu informacyjnego oraz zarządzania nim, a następnie przedstawiono dwa międzynarodowe standardy dotyczące bezpieczeństwa systemów informacyjnych. Artykuł prezentuje zakres tematyczny tych dokumentów, charakteryzuje główne zagadnienia oraz podaje przykłady kilku wytycznych.

Słowa kluczowe: system informacyjny, bezpieczeństwo, zarządzanie, ISO/IEC 17799, ISO/IEC 13335.

1. Wstęp

Każdy z nas kojarzy termin bezpieczeństwo z poczuciem braku zagrożenia, ze spokojem. Systemy informacyjne są narażone na różnego typu niebezpieczeństwa, począwszy od przestępstw dokonywanych za pomocą komputerów, poprzez sabotaż i szpiegostwo, a na aktach wandalizmu skończywszy. Rozwój nowoczesnych technologii, rozproszenie przetwarzania informacji oraz zarządzania sieciami stwarza nowe możliwości nieautoryzowanego dostępu do systemu [Andrukiewicz 1998]. Od poziomu bezpieczeństwa systemu informacyjnego zależeć może bardzo wiele aspektów działania przedsiębiorstwa. Kiedy system informacyjny firmy jest zagrożony, na niebezpieczeństwo narażone są również: zachowanie pozycji na rynku, konkurencyjność, płynność finansowa, sytuacja prawna czy wizerunek instytucji [Andrukiewicz 1998]. Zatem z jednej strony systemy informacyjne dają przedsiębiorstwom wiele korzyści, z drugiej jednak, niewłaściwie chronione, mogą zaszkodzić. Świadczy to o niezwykłej wadze bezpieczeństwa tych systemów. Celem niniejszego artykułu jest zaprezentowanie dwóch międzynarodowych standardów dotyczących zarządzania bezpieczeństwem systemu informacyjnego, a tym samym wskazanie, w jaki sposób można podnieść poziom bezpieczeństwa przetwarzania informacji w przedsiębiorstwie w niektórych obszarach.

2. Zarządzanie bezpieczeństwem systemu informacyjnego

Bezpieczeństwo systemu informacyjnego, czyli stan niezagrożenia i pewności jego elementów, możemy określić jako zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności oraz niezawodności, czyli atrybutów bezpieczeństwa [Andrukiewicz 1998; Białas 2007; Grzech 2008]. Podkreślić należy, że nie wszystkie atrybuty bezpieczeństwa odnoszą się do wszystkich elementów systemu. Część atrybutów, np. integralność, odnosi się do całego systemu, a część tylko do wybranych elementów, jak np. rozliczalność, która polega na weryfikowaniu wykorzystania systemu przez określone podmioty [Białas 2007]. Dokładniejszą charakterystykę tych atrybutów przedstawia tab. 1. Procesem umożliwiającym osiągnięcie stanu bezpieczeństwa jest zabezpieczenie systemu informacyjnego poprzez zdefiniowanie, osiągnięcie i utrzymanie stanu spełnienia kryteriów bezpieczeństwa [Andrukiewicz 1998].

Tabela 1. Atrybuty bezpieczeństwa

Nazwa	Określenie
Poufność	Właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom.
Autentyczność	Właściwość 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 czym, za kogo się podaje.
Dostępność	Właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez kogoś lub coś, co ma do tego prawo.
Integralność danych	Właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
Integralność systemu	Właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
Integralność	Integralność danych oraz integralność systemu.
Rozliczalność	Właściwość zapewniająca, że działania podmiotu (np. użytkownika) mogą być jednoznacznie przypisane tylko temu podmiotowi.
Niezawodność	Właściwość oznaczająca spójne, zamierzone zachowanie i skutki.

Źródło: PN-13335-1:1999, *Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych*.

Mając zdefiniowane pojęcie bezpieczeństwa systemu informacyjnego, możemy zdefiniować zarządzanie bezpieczeństwem systemu informacyjnego jako „zespół procesów zmierzających do osiągnięcia i utrzymywania ustalonego poziomu bezpieczeństwa, tzn. poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności" [Białas 2008]. Zarządzanie bezpieczeństwem systemu informacyjnego powinno obejmować następujące działania:

– określenie celów (co należy chronić), strategii (w jaki sposób) i polityki bezpieczeństwa systemów informatycznych w instytucji (jakie konkretne przedsięwzięcia należy podjąć),
– identyfikowanie i analizowanie zagrożeń zasobów,
– identyfikowanie i analizowanie ryzyka,
– określenie adekwatnych zabezpieczeń,
– monitorowanie wdrożenia i eksploatacji (skuteczności) zabezpieczeń,
– opracowanie i wdrożenie programu szkoleniowo-uświadamiającego,
– wykrywanie incydentów i reakcja na nie [ISO/IEC 27002:2005, *Technologia informacyjna…*].

Wytyczne co do realizacji wyżej wymienionych działań znajdują się m.in. w międzynarodowych standardach ISO/IEC 17799 oraz ISO/IEC 13335, które zostaną omówione poniżej.

3. ISO/IEC 17799

Standard ISO/IEC 17799 został opublikowany pod tytułem *Technologia informacyjna – techniki bezpieczeństwa – zbiór przepisów dotyczących zarządzania bezpieczeństwem informacji*. Dokument ten został przygotowany przez techniczny komitet ISO/IEC JTC 1. Obecna druga edycja ISO/IEC 17799:2005 unieważnia i zastępuje pierwszą ISO/IEC 17799:2000. Od 6 lipca 2007 r. standard ten dostępny jest pod nazwą ISO/IEC 27002:2005. Jest to dokładnie ten sam dokument, ale objęty nowym schematem numerowania. Zmianę, o której mowa, wprowadza sprostowanie ISO/IEC 17799:2005/Cor 1:2007, tak więc obecnie obowiązującym standardem jest ISO/IEC 27002:2005. Standard ustanawia wytyczne i generalne zasady inicjowania, wdrażania, utrzymywania i doskonalenia zarządzania bezpieczeństwem informacji w organizacji. Cele zawarte w dokumencie zarysowują zadania, jakie stoją przez zarządzaniem bezpieczeństwem informacji. Zagadnienia omawiane w ISO/IEC 27002 to:

1) definicje pojęć używanych w standardzie (rozdział 2),
2) oszacowanie ryzyka i postępowanie z nim (rozdział 4),
3) polityka bezpieczeństwa (rozdział 5),
4) organizacja bezpieczeństwa informacji (rozdział 6),
5) zarządzanie zasobami (rozdział 7),
6) bezpieczeństwo zasobów ludzkich (rozdział 8),
7) ochrona fizyczna i środowiskowa (rozdział 9),
8) zarządzanie komunikacją i obsługą (rozdział 10),
9) kontrola dostępu (rozdział 11),
10) nabywanie, rozwój i utrzymanie systemów informacyjnych (rozdział 12),
11) zarządzanie incydentami bezpieczeństwa informacji (rozdział 13),
12) zarządzanie ciągłością biznesową (rozdział 14),
13) zgodność (rozdział 15) [Streszczenie ISO/IEC 17799:2005…].

Opis każdej kategorii bezpieczeństwa w tym standardzie zawiera cele, jakie mają być osiągnięte, oraz środki, za pomocą których można je osiągnąć (zabezpieczenia). Dokładne omówienie wszystkich wytycznych zawartych w normie znacznie wykracza poza ramy tego artykułu, dlatego zostaną tu zaprezentowane tylko przykładowe kategorie bezpieczeństwa z rozdziałów 9 i 11 normy. W rozdziale 9 zostały wyszczególnione kategorie bezpieczeństwa dotyczące ochrony fizycznej i środowiskowej, a mianowicie:

1. Obszary bezpieczeństwa, wśród których wyróżniono:
– fizyczne ogrodzenie,
– fizyczną kontrolę dostępu,
– chronione biura, pokoje i środki przetwarzania,
– ochronę przed zagrożeniami zewnętrznymi i środowiskowymi,
– pracę w bezpiecznych obszarach,
– dostęp publiczny, dostawy i obszary załadunku.

2. Bezpieczeństwo sprzętu, które obejmuje takie problemy, jak:
– lokalizacja i ochrona,
– dostawcy mediów,
– bezpieczeństwo okablowania,
– utrzymanie sprzętu,
– bezpieczeństwo sprzętu poza siedzibą firmy,
– bezpieczne wycofanie sprzętu z użycia [Streszczenie ISO/IEC 17799:2005…].

Skupimy się teraz na ochronie przed zagrożeniami zewnętrznymi i środowiskowymi z grupy obszarów bezpieczeństwa. Celem implementacji takiej ochrony jest ochrona przed skutkami: pożaru, powodzi, trzęsienia ziemi, wybuchu, zamieszek ludności i innych klęsk naturalnych bądź spowodowanych przez człowieka. Szczegółowe wytyczne w tym zakresie proponują:
– zastanowienie się, czy w sąsiedztwie nie ma zagrożenia, np. pożarem czy zalaniem, z powodu których mogą ucierpieć nasze budynki,
– przechowywanie materiałów niebezpiecznych i łatwopalnych w bezpiecznej odległości od obszarów chronionych,
– przechowywanie w odpowiednich miejscach zapasowych kopii z danymi,
– utrzymywanie sprawności systemu gaśniczego [Streszczenie ISO/IEC 17799:2005…].

W drugiej grupie zabezpieczeń fizycznych i środowiskowych szczegółowo zostanie scharakteryzowane bezpieczeństwo sprzętu poza siedzibą firmy, a więc zabezpieczenie przed zagrożeniami, na które narażony jest sprzęt przenośny. Szczegółowe wytyczne przedstawiają się następująco:
– wydawanie zgody na używanie sprzętu poza siedzibą firmy przez kierownictwo,
– niepozostawianie sprzętu i nośników z danymi w miejscach publicznych bez nadzoru,

– przestrzeganie instrukcji bezpieczeństwa sprzętu, w szczególności tych dotyczących oddziaływania na nie promieniowania elektromagnetycznego,
– zabezpieczenie środowiska pracy w domu (oszacowanie ryzyka, odpowiednie środki ochronne),
– stosowanie ochrony ubezpieczeniowej [Streszczenie ISO/IEC 17799:2005…].

Rozdział 11 porusza natomiast tematykę kontroli dostępu, opisując zagadnienia takie, jak:

1) wymagania biznesowe co do kontroli dostępu, zawierające następujące podkategorie bezpieczeństwa:
– polityka kontroli dostępu;

2) zarządzanie dostępem użytkownika:
− rejestracja użytkownika,
− zarządzanie uprawnieniami,
− zarządzanie hasłami,
− przegląd praw dostępu;

3) obowiązki użytkownika:
− użycie hasła,
− sprzęt pozostawiony bez opieki,
− polityka czystego biurka i ekranu;

4) sieciowa kontrola dostępu:
− polityka używania usług sieciowych,
− autoryzacja użytkownika połączeń zewnętrznych,
− identyfikacja sprzętu w sieci,
− zdalne diagnozowanie i ochrona konfiguracji portów,
− segregacja w sieci,
− zabezpieczenie połączenia sieciowego,
− kontrola przekierowywania w sieci;

5) kontrola dostępu do systemu operacyjnego:
− bezpieczne procedury logowania,
− identyfikacja i autoryzacja użytkownika,
− system zarządzania hasłami,
− użycie narzędzi systemowych,
− automatyczna dezaktywacja sesji po przekroczeniu określonego czasu bezczynności,
− limitowanie czasu połączenia;

6) kontrola dostępu do aplikacji i informacji:
− ograniczenia w dostępie do informacji,
− izolowanie wrażliwych systemów;

7) usługi mobilne i telepraca:
− usługi mobilne i komunikacja,
− telepraca [Streszczenie ISO/IEC 17799:2005…].

Rozdział 11 również opisuje bardzo wiele zagadnień, dlatego przedstawione zostaną tylko przykładowe wytyczne. Skupimy się na obowiązkach użytkownika systemu informacyjnego. Najistotniejszą spośród nich kwestią jest używanie haseł. Celem tej podkategorii bezpieczeństwa jest wymuszenie na użytkownikach systemu odpowiedniego stosowania haseł. Standard wyszczególnia w tej dziedzinie następujące wytyczne:

– nieujawnianie haseł,
– nieprzechowywanie haseł poza specjalnie do tego przeznaczonymi i zaakceptowanymi systemami,
– zmiany haseł, kiedy istnieje podejrzenie, że mogło ono dostać się w niepowołane ręce,
– tworzenie odpowiednich jakościowo haseł (długość, liczność alfabetu – czyli ilość znaków w alfabecie, łatwość zapamiętania),
– okresowe zmiany haseł,
– niekorzystanie z zapamiętywania haseł w systemie,
– nieujawnianie haseł innym uprawnionym użytkownikom,
– niestosowanie tych samych haseł w celach prywatnych i biznesowych [Streszczenie ISO/IEC 17799:2005…].

4. ISO/IEC 13335

Standard ISO/IEC 13335 jest zatytułowany: *Technologia informacyjna – techniki bezpieczeństwa – zarządzanie bezpieczeństwem technologii informacyjnych i komunikacyjnych*. Składa się on z dwóch części:

1. *Koncepcje i modele dla zarządzania bezpieczeństwem technologii informacyjnej i komunikacyjnej (ICT)*[1].

2. *Techniki zarządzania ryzykiem bezpieczeństwa technologii informacyjnych i komunikacyjnych* (w przygotowaniu).

Dokument ISO/IEC 13335 jest opracowywany przez techniczny komitet ISO/IEC JTC 1. Pierwsza edycja ISO/IEC 13335-1 anuluje i zastępuje raporty techniczne ISO/IEC TR 13335-1:1996 oraz ISO/IEC TR 13335-2:1997. W momencie opublikowania drugiej części dokumentu ISO/IEC 13335-2 wycofane i zastąpione zostaną raporty techniczne ISO/IEC TR 13335-3:1998 i ISO/IEC TR 13335-4:2000. Wśród raportów technicznych ISO/IEC TR 13335 znajdowała się jeszcze piąta część, która została zastąpiona przez dokument ISO/IEC 18028-1:2006 [ISO/IEC 13335-1, *Information technology*...]. Głównym celem całego dokumentu ISO/IEC 18028, który składa się z pięciu części, jest rozszerzenie wytycznych zawartych w raportach technicznych ISO/IEC TR 13335 oraz w dokumencie ISO/IEC 17799. ISO/IEC 18028 dostarcza szczegółowych wytycznych w zakresie specyficznych operacji i mechanizmów niezbędnych do zaimplementowania bezpieczeństwa sieciowego. Dokument

[1] ICT – Information and Communication Technology.

integruje zarządzanie bezpieczeństwem IT oraz techniczne aspekty bezpieczeństwa [Streszczenie ISO/IEC 18028-1:2006…]. Poniżej zostaną omówione poszczególne, aktualne części dokumentu ISO/IEC 13335, a więc:

1. ISO/IEC 13335-1. Opisuje takie aspekty zarządzania, jak: planowanie, wdrażanie i działanie, włączając utrzymanie bezpieczeństwa ICT.

2. ISO/IEC TR 13335-3. Opisuje techniki zarządzania ryzykiem dotyczące bezpieczeństwa.

3. ISO/IEC TR 13335-4. Zawiera porady dotyczące wyboru zabezpieczeń [ISO/IEC 13335-1, *Information technology*...].

ISO/IEC 13335-1 dostarcza informacji ogólnych, dlatego wszystkich proponowanych wytycznych nie da się zaimplementować w każdej organizacji. W takiej sytuacji ważne jest, aby w danej organizacji zastosować odpowiednie wytyczne. Ta część dokumentu zawiera:

1) definicje pojęć używanych w całym standardzie (rozdział 2),

2) opisy głównych elementów bezpieczeństwa i związków pomiędzy nimi (rozdział 3),

3) cele, strategie i polityki niezbędne do realizacji bezpieczeństwa ICT (rozdział 4),

4) organizacyjne aspekty bezpieczeństwa ICT (rozdział 5),

5) przegląd funkcji zarządzania bezpieczeństwem ICT (rozdział 6) [ISO/IEC 13335-1, *Information technology*...].

W rozdziale 2 normy przedstawione są **definicje pojęć używanych w standardzie ISO/IEC 13335,** związanych z poruszaną tematyką. Wyjaśnione są tu następujące terminy: odpowiedzialność, zasób, autentyczność, dostępność, zabezpieczenia podstawowe, poufność, zabezpieczenie, wytyczne, wpływ, incydent bezpieczeństwa informacji, bezpieczeństwo ICT, polityka bezpieczeństwa ICT, podmioty przetwarzania informacji, bezpieczeństwo informacji, integralność, niezaprzeczalność, rzetelność, ryzyko, ryzyko rezydentne, analiza ryzyka, oszacowanie ryzyka, zarządzanie ryzykiem, postępowanie z ryzykiem, zagrożenie oraz podatność. Oprócz bardzo logicznego zdefiniowania powyższych zagadnień ten fragment pokazuje również ogólne związki pomiędzy poszczególnymi pojęciami. Za przykład może posłużyć definicja podatności, czyli słabości zasobu lub grupy zasobów, mogąca „być wykorzystana" przez jedno bądź więcej zagrożeń. Podatność jest definiowana za pomocą pojęć: zasób oraz zagrożenie, które także są wyjaśnione w powyższym słowniku [ISO/IEC 13335-1, *Information technology*...].

Rozdział 3 normy przedstawia **opisy głównych elementów bezpieczeństwa i związków pomiędzy nimi**. Standard wymienia następujące **zasady bezpieczeństwa**, stanowiące fundament programu ochrony ICT:

– zarządzanie ryzykiem: zasoby organizacji powinny być chronione poprzez zastosowanie odpowiednich zabezpieczeń, zabezpieczenia powinny być wybierane i należy nimi zarządzać na bazie odpowiedniej metodologii zarządzania ryzykiem, która to metodologia szacuje zasoby organizacji, zagrożenia, „podatności"

oraz ich wpływ; należy ustalić towarzyszące im ryzyko i wziąć pod uwagę ograniczenia;
– zaangażowanie: zaangażowanie organizacyjne w bezpieczeństwo ICT i zarządzanie ryzykiem są niezbędne; aby je uzyskać, powinny zostać wskazane korzyści z odpowiedniego rozlokowania bezpieczeństwa ICT;
– role i obowiązki: kierownictwo organizacyjne jest odpowiedzialne za ochronę zasobów, role i obowiązki dotyczące bezpieczeństwa ICT powinny zostać wyjaśnione i zakomunikowane;
– cele, strategie i polityka: zarządzanie ryzykiem powinno być realizowane z uwzględnieniem celów, strategii i polityki organizacji;
– zarządzanie cyklem życia: zarządzanie bezpieczeństwem ICT powinno być realizowane przez cały czas trwania cyklu życia chronionego zasobu.

W dalszej części rozdziału trzeciego normy scharakteryzowane są elementy zarządzania bezpieczeństwem oraz związki pomiędzy nimi, w odniesieniu do wcześniej zaproponowanych zasad. Do tych elementów możemy zaliczyć:
– zasoby,
– zagrożenia,
– „podatności”,
– wpływ,
– ryzyko,
– zabezpieczenia,
– ograniczenia [ISO/IEC 13335-1, *Information technology*...].

W standardzie został zaprezentowany model (rys. 1), który pokazuje związki i oddziaływania pomiędzy poszczególnymi elementami zarządzania bezpieczeństwem organizacji. W modelu znajdują odzwierciedlenie następujące elementy:
– środowisko, w którym działa organizacja wraz z ograniczeniami,
– zasoby organizacji,
– „podatności” powiązane z zasobami,
– zabezpieczenia wybrane w celu ochrony zasobów,
– ryzyko rezydentne, które organizacja jest w stanie zaakceptować.

Taki model posiada minimum pięć scenariuszy realizacji, które można opisać w następujący sposób:

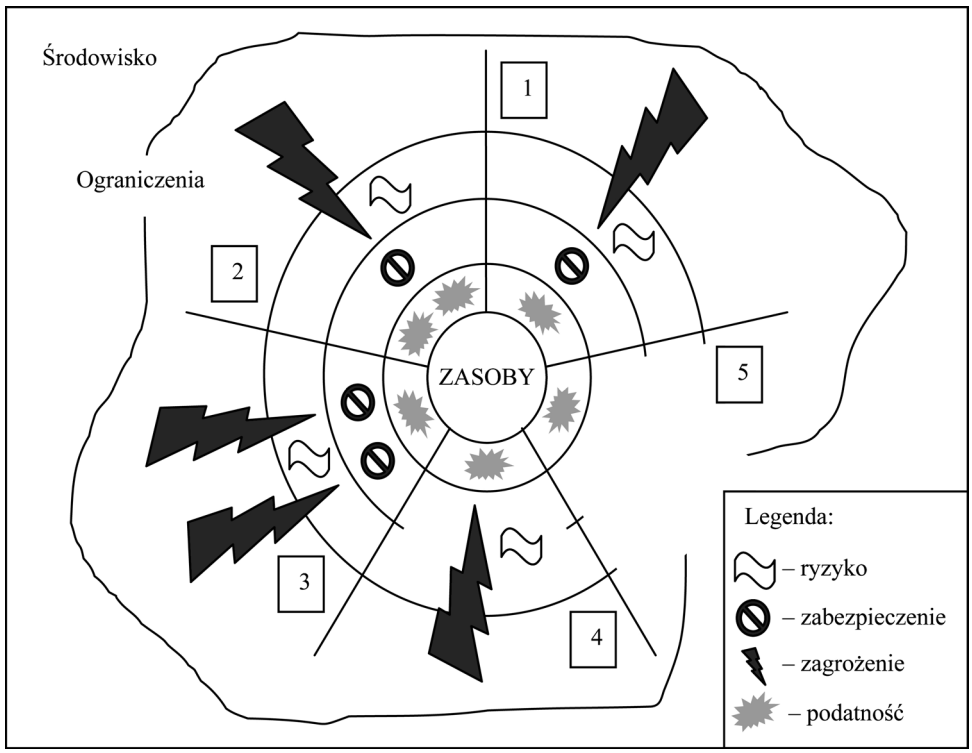
1. Scenariusz 1. Zabezpieczenie może skutecznie redukować ryzyko związane z realizacją zagrożenia zdolnego do „wykorzystania” podatności zasobu. Realizacja zagrożenia jest możliwa tylko w przypadku, kiedy zasób jest na nie podatny.

2. Scenariusz 2. Zabezpieczenie może skutecznie redukować ryzyko związane z realizacją zagrożenia „wykorzystującego” wiele „podatności”.

3. Scenariusz 3. Wiele zabezpieczeń może skutecznie redukować ryzyko związane z realizacją wielu zagrożeń. Czasami istnieje potrzeba kilku zabezpieczeń, aby obniżyć ryzyko do poziomu akceptowalnego.

4. Scenariusz 4. Ryzyko jest na akceptowalnym poziomie. Żadne zabezpieczenia nie są zaimplementowane, nawet jeśli obecne są zagrożenia oraz jeśli istnieją „podatności”.

5. Scenariusz 5. Istnieje podatność, ale nie są znane zagrożenia, które mogłyby ją wykorzystać.



Rys. 1. Powiązania pomiędzy elementami bezpieczeństwa

Źródło: opracowanie własne na podstawie [ISO/IEC 13335-1, *Information technology*…].

Centralnym punktem przedstawionego modelu są zasoby organizacji (na potrzeby niniejszej pracy skupiamy się głównie na zasobach informacyjnych), które mają dla niej określoną wartość. Zasoby te mogą być podatne na pewne zagrożenia, a więc charakteryzować się podatnością. Określone zagrożenie może „wykorzystać" z pewnym prawdopodobieństwem (ryzyko) daną podatność i w ten sposób wpłynąć negatywnie na dany zasób, a co za tym idzie – na funkcjonowanie przedsiębiorstwa. Zarówno wartość zasobu, jak i zagrożenia oraz podatność na nie mogą zwiększać ryzyko. Za pomocą oszacowania ryzyka możliwe jest wyznaczenie wymagań bezpieczeństwa, które spełniane są poprzez implementację zabezpieczeń. Zastosowanie zabezpieczeń odpowiednich do zagrożeń może zmniejszyć ryzyko realizacji zagrożenia, ochronić przed zagrożeniami oraz zredukować podatność [ISO/IEC 13335-1, *Information technology*...].

Cele, strategie i polityki niezbędne do realizacji bezpieczeństwa ICT zostały przedstawione w rozdziale 4 normy. Standard wyszczególnia ogólne zasady tworzenia celów, strategii i polityk bezpieczeństwa. Należą do nich:
– hierarchia definiowania,
– uwzględnianie wymagań organizacyjnych oraz ograniczeń,
– stosowanie podejścia całościowego (tworzenie celów, strategii i polityk we wszystkich obszarach działalności instytucji),
– okresowe aktualizowanie dokumentacji [ISO/IEC 13335-1, *Information technology*...].

Organizacyjne aspekty bezpieczeństwa ICT, przedstawione w rozdziale piątym standardu, wskazują na kolejną istotną kwestię dotyczącą zarządzania bezpieczeństwem, jaką są role i obowiązki. Aby zarządzanie bezpieczeństwem było efektywne, wymagane jest wyraźne przypisanie ról i obowiązków dotyczących bezpieczeństwa odpowiednim podmiotom. W każdej organizacji, niezależnie od wielkości czy struktury, powinny zostać ustanowione następujące role:
– forum bezpieczeństwa ICT, które będzie rozwiązywało problemy interdyscyplinarne, doradzało i rekomendowało strategie oraz zatwierdzało polityki i procedury działania;
– szef bezpieczeństwa ICT, który będzie czuwał nad wszystkimi aspektami dotyczącymi bezpieczeństwa w całej organizacji [ISO/IEC 13335-1, *Information technology*...].

Przegląd funkcji zarządzania bezpieczeństwem ICT zaprezentowany został w rozdziale szóstym. Wyszczególnione zostały działania, które powinny być cyklicznie wykonywane w organizacji w ramach poszczególnych funkcji zarządzania bezpieczeństwem. W obrębie planowania zarządzania bezpieczeństwem powinno się:
– wyznaczyć wymagania bezpieczeństwa,
– wyznaczyć, cele, strategie i polityki bezpieczeństwa,
– zidentyfikować role i obowiązki dotyczące bezpieczeństwa,
– rozwijać plan bezpieczeństwa,
– przeprowadzać oszacowanie ryzyka,
– podejmować decyzje dotyczące postępowania z ryzykiem i wybierać zabezpieczenia,
– planować ciągłość biznesową.

W ramach implementacji zarządzania bezpieczeństwem standard zaleca:
– implementować zabezpieczenia,
– zatwierdzać systemy ICT,
– rozwijać i implementować programy świadomościowe dotyczące bezpieczeństwa,
– dokonywać rewizji oraz monitorować wdrażanie zabezpieczeń.

W kwestii utrzymania zarządzania bezpieczeństwem należy:
– zarządzać konfiguracją i zmianami,

– zarządzać ciągłością biznesową,
– przeprowadzać rewizje, audyty, monitoring oraz sprawdzać zgodność bezpieczeństwa,
– zarządzać incydentami bezpieczeństwa informacji [ISO/IEC 13335-1, *Information technology*...].

Część druga standardu ISO/IEC 13335, czyli **ISO/IEC TR 13335-3:1998**, opisuje techniki zarządzania bezpieczeństwem w nawiązaniu do działań podejmowanych w ramach zarządzania cyklem życia projektu, takich jak: planowanie, projektowanie, implementowanie, testowanie, nabywanie, obsługa. Proponowane techniki oparte są na głównych wytycznych podanych w części pierwszej dokumentu i mają pomagać we wdrażaniu bezpieczeństwa IT. W kolejnych rozdziałach omawiane są następujące zagadnienia:

1) ogólne omówienie procesu zarządzania bezpieczeństwem IT (rozdział 6),
2) istota polityki bezpieczeństwa oraz co powinien zawierać taki dokument (rozdział 7),
3) cztery metody identyfikacji wymagań bezpieczeństwa (rozdział 8),
4) szczegółowe omówienie zalecanej metody (rozdział 9),
5) opis wdrażania zabezpieczeń (rozdział 10),
6) opis czynności, które zagwarantują efektywne działanie zabezpieczeń (rozdział 11),
7) podsumowanie całej części drugiej standardu (rozdział 12) [ISO/IEC 13335-3:1998, *Information technology*...].

Część trzecia z rodziny ISO/IEC 13335, czyli raport techniczny **ISO/IEC TR 13335-4:2000** dostarcza doradztwa w zakresie wyboru zabezpieczeń. Dokument określa także, jak selekcja zabezpieczeń może być wspierana poprzez użycie podstawowych modeli i zabezpieczeń oraz jak uzupełnia ona techniki bezpieczeństwa opisywane w części drugiej. Wytyczne zawarte w tej części wskazują również na dodatkowe metody oszacowania, które mogą być używane przy wyborze zabezpieczeń. W poszczególnych rozdziałach tej części standardu omawiane są następujące kwestie:

1) wprowadzenie do wyboru zabezpieczeń oraz do koncepcji ochrony podstawowej (rozdział 6),
2) podstawowe oszacowania niezbędne do wyboru odpowiednich zabezpieczeń (rozdział 7),
3) przegląd zabezpieczeń do wyboru; zabezpieczenia zostały podzielone na dwie grupy: organizacyjne i fizyczne oraz specyficzne dla systemów informacyjnych (rozdział 8),
4) specyfikacja zabezpieczeń odpowiednich dla konkretnych systemów informacyjnych (rozdział 9),
5) wybór zabezpieczeń w wypadku wnikliwej analizy obaw dotyczących bezpieczeństwa (rozdział 10),
6) wybór zabezpieczeń w sytuacji szczegółowej analizy ryzyka (rozdział 11),

7) stworzenie katalogu ochrony podstawowej dla całej organizacji lub jej części (rozdział 12),

8) podsumowanie całej części trzeciej (rozdział 13) [ISO/IEC TR 13335-4:2000, *Information technology*...].

Jak to zostało powyżej przedstawione, standard ISO/IEC 13335 obejmuje bardzo szerokie spektrum zagadnień związanych z bezpieczeństwem systemów informacyjnych. Tak jak w przypadku normy ISO/IEC 17799, omówienie wszystkich wykracza poza ramy tego artykułu, dlatego jako przykładowe wytyczne zostaną zaprezentowane działania uzupełniające implementację zabezpieczeń. Wdrożone zabezpieczenia mogą funkcjonować efektywnie tylko wtedy, gdy są sprawdzane w realnym środowisku. Jest to głównym zadaniem działań uzupełniających, które możemy podzielić na następujące grupy:

– administrowanie,
– sprawdzanie zgodności,
– zarządzanie zmianami,
– monitorowanie,
– postępowanie z incydentami [ISO/IEC TR 13335-4:2000, *Information technology*...].

Wiele zabezpieczeń wymaga ciągłego **administrowania**, aby mogły efektywnie spełniać założone funkcje. Następujące działania powinny być zaplanowane i regularnie przeprowadzane:

– sprawdzanie plików dziennika,
– modyfikowanie konfiguracji, aby reagować na zmiany i nowe elementy,
– ponowne definiowanie wartości początkowych,
– aktualizowanie do najnowszych wersji.

Sprawdzanie zgodności polega na rewizji i analizie zaimplementowanych zabezpieczeń. Ma to na celu sprawdzenie, czy systemy bądź usługi IT są zgodne z wymaganiami bezpieczeństwa. Może zostać przeprowadzone po zaimplementowaniu nowego systemu lub usługi – przez personel wewnętrzny lub zewnętrzny. **Zarządzanie zmianami** polega na dostosowywaniu wymagań bezpieczeństwa do aktualnych uwarunkowań. W systemie IT mogą się pojawić następujące zmiany:

– nowe procedury,
– nowe cechy,
– aktualizacje oprogramowania,
– rewizje sprzętu,
– nowi użytkownicy,
– dodatkowe, nowe połączenia.

Wszystkie te zmiany mogą wprowadzać nowe cechy i usługi, ale również stwarzać nowe zagrożenia i „podatności". Dlatego w firmie potrzebny jest efektywny proces reagowania na zmiany.

Kolejnym działaniem uzupełniającym jest **monitorowanie**, czyli ciągłe sprawdzanie, czy system, jego użytkownicy i środowisko, w którym działa, utrzymuje

poziom bezpieczeństwa zakładany przez plan bezpieczeństwa. **Postępowanie z incydentami** wymaga wdrożenia przez organizację schematu analizy incydentów IAS[2]. Informacje o incydentach powinny być przez organizację gromadzone i analizowane, tak aby mogły wspierać analizę ryzyka i inne działania dotyczące bezpieczeństwa [ISO/IEC 13335-3:1998, *Information technology…*].

5. Zakończenie

Zarządzanie bezpieczeństwem systemu informacyjnego jest niewątpliwie istotnym elementem funkcjonowania współczesnego przedsiębiorstwa, w którym informacje przetwarzane są z wykorzystaniem techniki komputerowej. Skomputeryzowane systemy informacyjne przynoszą firmom wiele wymiernych efektów, jednak w miarę wzrostu korzyści płynących z zastosowania nowoczesnych technologii rośnie podatność systemów na zagrożenia. Aby uchronić zasoby informacyjne przed utratą lub nieautoryzowanym ujawnieniem, trzeba podjąć odpowiednie działania, mające na celu eliminację zagrożeń lub zmniejszenie podatności systemu na zagrożenia – temu służą zaprezentowane dokumenty.

Jak pokazują badania przeprowadzone w amerykańskich przedsiębiorstwach, najchętniej i najczęściej stosowane są zabezpieczenia najtańsze i najłatwiejsze do wdrożenia. Oprogramowanie antywirusowe jest stosowane przez ponad 98% badanych firm, a zapory ograniczające przez nieco ponad 90%. Im bardziej złożona lub kosztowna jest implementacja danego zabezpieczenia, tym mniej firm z niego korzysta. Często również niewielki odsetek wykorzystania danej technologii zabezpieczeń wynika z braku świadomości zagrożeń. Na przykład zabezpieczenia pamięci przenośnych stosuje tylko niecałe 7% badanych firm [*2005 FBI Computer…*, s. 5].

Problem zarządzania bezpieczeństwem systemu informacyjnego nie powinien być traktowany wybiórczo. Skutecznej ochrony nie zapewni zastosowanie jedynie zabezpieczeń programowych. Do zagadnienia należy podejść całościowo, implementując zabezpieczenia programowe, techniczne, fizyczne oraz, co najważniejsze, administracyjno-organizacyjne. O złożoności tego problemu świadczy duża liczba zagadnień zawartych w prezentowanych standardach oraz ich szeroki zakres.

Literatura

2005 FBI Computer Crime Survey, www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf.

Andrukiewicz E., *Bezpieczeństwo systemów informacyjnych (1): Terminologia i nie tylko*, „PCkurier" 1998, nr 25.

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2007.

[2] IAS – Incident Analysis Scheme.

Białas A., *Zarządzanie bezpieczeństwem informacji*, http://www.networld.pl/artykuly/ artykul.asp?id=8098&w=1 (4.03.2008).

Grzech A., *Bezpieczeństwo systemu informatycznego*, www.biznesnet.pl/files/tmt4/ Adam_Grzech.ppt.ppt (4.03.2008).

ISO/IEC 13335-1, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*.

ISO/IEC 13335-3:1998, *Information technology – Guidelines for the management of IT security – Part 3: Techniques for the management of IT security*.

ISO/IEC 27002:2005, *Technologia informacyjna – Techniki bezpieczeństwa – Zbiór przepisów dotyczących zarządzania bezpieczeństwem informacji*.

ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards*.

Streszczenie ISO/IEC 17799:2005, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_ detail.htm?csnumber=39612 (8.05.2008).

Streszczenie ISO/IEC 18028-1:2006, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_ detail.htm? csnumber=40008 (5.05.2008).

INFORMATION SYSTEM SECURITY MANAGEMENT IN THE INTERNATIONAL STANDARDS ISO/IEC 17799 AND ISO/IEC 13335

Summary: The impact of the new technologies on the information systems security is significant. So we must maintain the information systems security on a appropriate level. At first there are defined the ideas of the information system security and the information system security management in this article. Afterwards there are presented two international documents (ISO/IEC 17799 and ISO/IEC 13335). This presentation contains scope of the documents, characteristic of the main issues and several examples of particular guidelines.