STUDIA I PRACE WYDZIAŁU NAUK EKONOMICZNYCH I ZARZĄDZANIA NR 16

Mariusz Prawicki

METODYKA AUDYTU WEWNĘTRZNEGO Z ZAKRESU BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH NA PRZYKŁADZIE URZĘDÓW SKARBOWYCH WOJEWÓDZTWA ZACHODNIOPOMORSKIEGO

Wprowadzenie

Zapewnienie bezpieczeństwa instytucji związanego z funkcjonowaniem środowiska informatycznego wymaga zastosowania odpowiednich zasad ochrony fizycznej, logicznej i wdrożenia mechanizmów wykonywania działalności zgodnie z obowiązującym prawem. Zabezpieczenia i metody nadzoru nad ich funkcjonowaniem muszą być dobierane w sposób optymalny, tak aby koszty poniesione na ich implementację i system kontroli ich działania miały odzwierciedlenie w efektach biznesowych instytucji.

Ważną kwestią jest właściwa organizacja systemu informatycznego oraz właściwe dobranie celów kontroli i mierników wskazujących rzeczywistą jakość zabezpieczeń.

Celem artykułu jest przedstawienie metodyki prowadzenia audytu wewnętrznego z zakresu bezpieczeństwa systemu informatycznego. Jako przykład został przedstawiony przebieg audytu realizowanego w urzędach skarbowych województwa zachodniopomorskiego.

1. Bezpieczeństwo systemów informatycznych

Bezpieczeństwo systemów informatycznych można ująć w ramach trzech głównych domen: bezpieczeństwa fizycznego, bezpieczeństwa logicznego oraz bezpieczeństwa prawnego.

Bezpieczeństwo fizyczne wiąże się z zapewnieniem bezpieczeństwa całej infrastruktury, dokumentów, informacji oraz personelu przed bezpośrednim dostępem osób nieuprawnionych, zniszczeniem, uszkodzeniem, zranieniem.

Zapewnienie bezpieczeństwa fizycznego wymaga zastosowania środków przeciwdziałających zagrożeniom związanym z[1]:

– działaniem czynników środowiskowych,
– terroryzmem,
– zapewnieniem dostaw mediów,
– niewłaściwym użytkowaniem infrastruktury,
– dostępem do infrastruktury osób nieuprawnionych.

Ze względu na położenie geograficzne Polski zagrożenia ze strony **czynników środowiskowych** są stosunkowo niewielkie. Znikome jest prawdopodobieństwo huraganu, niewielkie wstrząsy sejsmiczne, a wstrząsy będące skutkami prac górniczych występują głównie na terenie Polski południowej. Z zagrożeń środowiskowych największym jest zagrożenie powodziami i podtopieniami. Przeciwdziałaniem jest przede wszystkim właściwa lokalizacja obiektów.

Sporadycznie mogą wystąpić również inne zagrożenia środowiskowe, na przykład anomalie pogodowe, których skutki będą odczuwalne w pracy firm, administracji i funkcjonowaniu gospodarstw domowych. Przykładem może tu być silny opad bardzo mokrego śniegu, który miał miejsce w kwietniu 2008 roku i spowodował uszkodzenie wszystkich linii energetycznych zasilających Szczecin, a w następstwie tego paraliż funkcjonowania miasta i okolic na wiele godzin.

Czynnikiem o rosnącym znaczeniu jest **zagrożenie terrorystyczne**. Wraz ze wstąpieniem do NATO i zaangażowaniem Polski w działania w Iraku i Afganistanie zwiększyło się prawdopodobieństwo dokonania ataku terrorystycznego na terenie naszego kraju.

[1] Forystek M., *Audyt informatyczny*, InfoAudit Sp. z o.o., Warszawa 2005, s. 109.

Ważnym elementem bezpieczeństwa jest zapewnienie **dostawy mediów**. Niewątpliwie podstawowe znaczenie ma dostawa energii elektrycznej, od której zależy funkcjonowanie praktycznie wszystkich firm, instytucji i gospodarstw domowych.

Zagrożenie dla urządzeń elektrycznych stanowi nie tylko brak zasilania, który uniemożliwia ich pracę, ale również zmienne parametry zasilania (skoki napięcia, przenoszenie siecią impulsów elektrycznych, zmiany częstotliwości prądu elektrycznego), które mogą doprowadzić do nieprawidłowego działania, uszkodzenia lub zniszczenia urządzeń podłączonych do sieci elektrycznej.

Brak zasilania niewątpliwie pogorszy również ochronę fizyczną obiektów ze względu na zaprzestanie działania instalacji alarmu przeciwpożarowego, alarmu antywłamaniowego, telewizji przemysłowej, systemu elektronicznej kontroli dostępu. Część systemów ma zapewnione zasilanie awaryjne, ale czas jego działania jest ograniczony.

Dużym zagrożeniem jest zakłócenie dostaw gazu. Ze względu na prawdopodobieństwo pozostawienia otwartych zaworów gazu w przypadku jego braku, wzrośnie prawdopodobieństwo pożarów i wybuchów po wznowieniu dostaw.

Pewnym zagrożeniem jest również możliwość naruszenia działania sieci wodociągowej i kanalizacyjnej. Brak wody lub brak odprowadzania ścieków nie uniemożliwi w sposób natychmiastowy pracy większości firm i instytucji, lecz w miarę upływu czasu staje się coraz bardziej uciążliwy, a pogorszenie warunków pracy wpłynie negatywnie na ilość i jakość wykonywanych zadań oraz zwiększy podatność na ataki skierowane na czynnik ludzki.

Największym zagrożeniem i to nie tylko dla funkcjonowania, ale i istnienia każdej firmy i instytucji, jest **pożar**. Przyczyny jego powstania mogą być różne – zaprószenie ognia, zwarcie w instalacji, przeniesienie się ognia z obiektu palącego się w pobliżu, uderzenie pioruna, atak terrorystyczny. Jednakże bez względu na przyczynę powstania pożaru, skutki mogą doprowadzić do takiego samego efektu – nawet doszczętnego spalenia całej infrastruktury i utraty wszystkich danych oraz znacznej części personelu.

Poważnym zagrożeniem może być również **niewłaściwe użytkowanie** elementów infrastruktury. Przykładami niewłaściwego użytkowania są: stawianie napojów lub żywności w pobliżu klawiatury lub na komputerze, stawianie napojów lub żywności na macierzach dyskowych, serwerach, urządzeniach telekomunikacyjnych, urządzeniach zamontowanych w szafach krosowych, używanie urządzeń niezgodnie

z zaleceniami producenta, ustawianie urządzeń w niewłaściwej kolejności jedno na drugim, wystawianie urządzeń lub nośników informacji na działanie promieni słonecznych lub mrozu, a w przypadku niektórych urządzeń niewłaściwa kolejność ich włączania i wyłączania.

Istotne zagrożenia wiążą się z **dostępem do elementów infrastruktury i dokumentów**. Szczególnie okres kryzysu i zagrożenia bezpieczeństwa państwa oraz okresy niepokojów społecznych sprzyjają próbom uzyskania nieuprawnionego fizycznego dostępu do pomieszczeń, urządzeń i informacji w celu kradzieży, rabunku, dywersji lub szpiegostwa.

Najsłabszym elementem systemu jest zazwyczaj człowiek i w tym kierunku idzie wiele działań agresorów. Wykorzystywany jest tak zwany *social engineering* – czyli próby manipulacji ludźmi w celu uzyskania określonych celów.

Zapewnienie właściwego bezpieczeństwa fizycznego wspomaga właściwa organizacja obszarów o różnych prawach dostępu. Wskazane jest wydzielenie strefy administracyjnej i stref bezpieczeństwa.

Nie należy również zapominać o sposobie oznaczania pomieszczeń. Dla pomieszczeń szczególnie chronionych, jakimi niewątpliwie są pomieszczenia zakwalifikowane jako strefy bezpieczeństwa, zalecana jest[2] rezygnacja z wszelkich tabliczek identyfikacyjnych na drzwiach oraz nieumieszczanie numerów telefonów w ogólnodostępnych spisach.

Bezpieczeństwo logiczne wiąże się z zapewnieniem zabezpieczenia systemu informatycznego przed nieautoryzowanym dostępem osób nieuprawnionych i wykorzystaniem go do ujawnienia, zniekształcenia lub zniszczenia informacji znajdujących się w tym systemie przy wykorzystaniu narzędzi technicznych, w tym informatycznych[3].

Dostęp logiczny powinien zawsze opierać się na zasadzie „wiedzieć tylko to, co konieczne". Przyznanie niewłaściwych praw dostępu oznacza ryzyko wystąpienia wielu zagrożeń i może być wykorzystany w celu: sabotażu, szpiegostwa, szantażu oraz osiągnięcia bezpośrednich lub pośrednich korzyści finansowych.

Należy zwrócić uwagę, że z luk w mechanizmach kontroli dostępu logicznego korzystają nie tylko intruzi zewnętrzni, ale bardzo często, a statystyki wskazują, że wręcz najczęściej, osoby z wewnątrz organizacji.

[2] Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999, s. 47.

[3] M. Forystek, *Audyt informatyczny*..., s. 37.

Szczególną uwagę należy tu poświęcić pracownikom. Mogą oni wykonać szereg działań na szkodę organizacji zarówno wykorzystując prawidłowo nadane uprawnienia, przed czym ochrona jest trudna, jak i zbyt szeroko nadane uprawnienia.

O zastosowanych środkach kontroli dostępu logicznego decyduje przeznaczenie chronionego systemu i znaczenie chronionych informacji. W systemie informatycznym użytkownik identyfikowany jest przez nadany mu identyfikator. Identyfikator użytkownika jest wykorzystywany przy ustalaniu praw dostępu użytkownika do zasobów oraz służy jako ścieżka audytu przy ustalaniu wykonywanych przez niego operacji w systemie informatycznym.

Do autoryzacji użytkownika najczęściej wykorzystywane jest hasło. Jest ono zastępowane, bądź też uzupełniane, innymi metodami autoryzacji, na przykład:
– kartami magnetycznymi lub procesorowymi,
– tokenami,
– czytnikami parametrów biometrycznych.

Ze względu na fakt, iż w większości przypadków do autoryzacji użytkownika stosowane jest hasło, należy zwrócić szczególną uwagę na zasady jego tworzenia, przechowywania i użytkowania. Zasady te należy dostosować do stopnia ochrony wymaganego przez systemy i dane, do których uzyskuje się dostęp w wyniku autoryzacji. W niektórych przypadkach wymagania są określone w przepisach prawa powszechnego, jak na przykład w przypadku danych osobowych[4]. W innych przypadkach wymagania regulowane są przez przepisy prawa wewnętrznego lub instytucje certyfikujące systemy.

Zapewnienie właściwego stopnia bezpieczeństwa logicznego wymaga wdrożenia mechanizmów kontrolujących realizację zasad zawartych w politykach bezpieczeństwa i wdrożenie stosowania obowiązujących procedur.

Bezpieczeństwo prawne systemów informatycznych związane jest ze zgodnym z prawem funkcjonowaniem systemu informatycznego. Bezpieczeństwo prawne systemów informatycznych rozpatrywać można w aspektach:
– legalności stosowanego oprogramowania,
– zgodności z prawem w zakresie przetwarzania danych.

[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, DzU nr 100, poz. 1024.

Bezpieczeństwo prawne jest często sprowadzane do pierwszego elementu – zapewnienia legalności stosowanego oprogramowania. Wiele firm oferujących audyty informatyczne w rzeczywistości oferuje wyłącznie inwentaryzację oprogramowania. Legalność używanego oprogramowania jest zagadnieniem bardzo ważnym, ale jest jedynie cząstką bezpieczeństwa prawnego.

Problem legalności oprogramowania spowodowany może być nie tylko zamierzoną kradzieżą własności intelektualnej, lecz również niewłaściwym zarządzaniem licencjami.

Ograniczenia licencyjne mogą być związane z wieloma aspektami funkcjonowania i składnikami systemu informatycznego. Mogą to być:
– ilość użytkowników,
– ilość procesorów (przy czym w procesorach wielordzeniowych każdy rdzeń może być traktowany jako osobny procesor),
– ilość podłączonych równocześnie klientów,
– ograniczenie czasowe używania programu,
– ograniczenie wielkości obsługiwanych zasobów (na przykład wielkość pliku bazy danych),
– ilość stanowisk, na których program może zostać zainstalowany,
– ilość stanowisk, na których program może być równocześnie używany.

Zarządzanie licencjami utrudnia fakt, że licencja do każdego programu jest inna, wprowadza inne ograniczenia i najczęściej podawana jest w języku angielskim.

Osobne zagadnienie stanowi **zgodne z prawem przetwarzanie danych**. Mnogość aktów prawnych, które definiują i określają zasady postępowania w zakresie ochrony informacji w zależności od jej rodzaju, może spowodować sytuację, w której użytkownik nie jest świadomy, że podejmowane przez niego działania mogą podlegać regulacjom prawnym[5]. Regulacje prawne odnoszące się do ochrony informacji znaleźć można w aktach prawnych z zakresu:
– ochrony danych osobowych,
– ochrony informacji niejawnych,
– ochrony baz danych,

[5] J. Radziulis, W. Hołubowicz, *Wymagania dotyczące bezpieczeństwa informacji i baz danych zawarte w obowiązujących w Polsce aktach prawnych*, XII Konferencja PLOUG, Zakopane 2006, s. 237, www.ploug.org.pl.

– ochrony dokumentacji księgowej,
– informatyzacji działalności podmiotów realizujących zadania publiczne,
– świadczenia usług drogą elektroniczną,
– elektronicznych instrumentów płatniczych,
– podpisu elektronicznego,
– ochrona tajemnicy telekomunikacyjnej,
– postępowania z materiałami archiwalnymi,
– ochrony tajemnicy skarbowej,

przy czym nie jest to lista zamknięta.

Należy zwrócić uwagę, że terminologia odnosząca się do ochrony informacji stosowana w aktach prawnych dotyczących różnych dziedzin nie jest spójna, a zakres i szczegółowość uregulowań są różne.

Zapewnienie właściwego stopnia bezpieczeństwa systemu informatycznego wymaga stosowania odpowiednio dobranych środków budujących bezpieczeństwo fizyczne i logiczne z uwzględnieniem wymogów stawianych przez przepisy prawa.

2. Metodyka audytu informatycznego w świetle obowiązujących przepisów i standardów

Metodyka przeprowadzania audytu wewnętrznego jest w Polsce uregulowana przez przepisy prawa. Obowiązek i sposób przeprowadzania audytu wewnętrznego reguluje ustawa o finansach publicznych[6] i rozporządzenie Ministra Finansów w sprawie szczegółowego sposobu i trybu przeprowadzania audytu wewnętrznego[7].

Jednakże przepisy prawa nie porządkują osobno metodyki przeprowadzania audytu wewnętrznego w tym szczególnym zakresie, jakim jest audyt systemów informatycznych. W celu ułatwienia organizacji zarządzania systemem informatycznym i jego kontroli zostały opracowane metodyki dostosowane do specyfiki środowiska informatycznego. Są to opracowania wykonane zarówno przez polskich autorów (na przykład LP-A, TISM), jak i przez duże nieraz zespoły międzynarodowe (na przy-

[6] Ustawa z dnia 30 czerwca 2005 o finansach publicznych, DzU nr 249, poz. 2104, z późn. zm.

[7] Rozporządzenie Ministra Finansów z dnia 10 kwietnia 2008 roku w sprawie sposobu i trybu przeprowadzania audytu wewnętrznego, DzU nr 66, poz. 406.

kład COBIT). Metodyki te różnią się zarówno zakresem objętych nimi zagadnień, jak i bardzo nieraz odmiennym podejściem do tematu.

Metodyka LP-A[8] przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego została opracowana przez Krzysztofa Lidermana i Adama E. Patkowskiego z Instytutu Teleinformatyki i Automatyki Wojskowej Akademii Technicznej. Metodyka dotyczy przeprowadzania audytu systemów i sieci teleinformatycznych służących do realizacji prac biurowych, przetwarzania baz danych, nie dotyczy natomiast systemów automatyki przemysłowej i sterowania.

Metodyka LP-A określa skład zespołu audytowego, kwalifikacje jego członków i zakresy kompetencji. Opisane jest również wyposażenie narzędziowe zespołu audytowego, na które składają się następujące elementy:

– kwestionariusze ankietowe opracowane na podstawie zaleceń normy ISO/IEC 17799 składające się z 913 szczegółowych pytań dotyczących dziesięciu grup tematycznych,
– szablony edycyjne dokumentów wspomagające tworzenie dokumentów zgodnie z ustalonym schematem i umieszczonymi właściwie treściami,
– narzędzia zautomatyzowane – programy komputerowe (skanery bezpieczeństwa, skanery inwentaryzacyjne, skanery konfiguracji).

Zweryfikowana na podstawie wywiadów i wizji lokalnych ankieta stanowi podstawę do oceny spełniania wymagań 139 wynikających z normy ISO/IEC 17799 punktów audytowych.

Cechą charakterystyczną metodyki LP-A jest realizacja, obok badanego w ramach ścieżki formalnej stopnia zgodności sposobu zarządzania bezpieczeństwem teleinformatycznym z przyjętym wzorcem na podstawie analizy dokumentacji, wizji lokalnych i wywiadów, również przeprowadzenie w ramach ścieżki technicznej badań systemów ochrony fizycznej i technicznej oraz sieci i systemów teleinformatycznych objętych zadaniem audytowym.

Metodyka zarządzania bezpieczeństwem informacji **TISM**[9] (skrót od nazwy w języku angielskim *Total Information Security Management*) została opracowana

[8] K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa 2003, s. 291–328.

[9] M. Byczkowski, P. Marciniak, *TISM – Total Information Security Management*, Dokumentacja ver. 1.4 RC1, www.ensi.net.

przez polską firmę ENSI (*European Network Security Institute*). Jest udostępniana na zasadzie licencji „*GNU Free Documentation License*".

Metodyka TISM pozwala zbudować modułową i hierarchiczną Politykę Bezpieczeństwa Informacji, dzięki której można łatwo zarządzać bezpieczeństwem różnych grup informacji. Wiodącym celem metodyki jest stworzenie konkretnej struktury zarządzania, czyli określenie ról zarządzających i kontrolnych, niezbędnych dla podtrzymania procesów ochrony informacji. Wdrażana Polityka Bezpieczeństwa Informacji określa podstawowe zasady ochrony informacji, niezależnie od systemów ich przetwarzania (informatyczny, papierowy) oraz sposobu ich przetwarzania w tych systemach. Podstawą jest opracowanie szczegółowych założeń bezpieczeństwa jakie muszą spełniać systemy, w których informacje chronione są lub będą przetwarzane, jak również określenie praw, obowiązków i odpowiedzialności osób dopuszczonych do informacji chronionych.

Struktura dokumentacji bezpieczeństwa tworzonej zgodnie z metodyką TISM jest hierarchiczna. Dokumentem nadrzędnym jest Polityka Bezpieczeństwa Informacji. Z niej wynika konieczność stworzenia pozostałych dokumentów:
- polityk dla grup informacji chronionych,
- polityk dla systemów przetwarzania,
- procedur dla systemów przetwarzania,
- regulaminów.

Metodyka TISM przewiduje wykonanie audytu na dwóch etapach wdrażania. Audyt bezpieczeństwa grup przetwarzanych informacji służy dostosowaniu systemów przetwarzania do wymogów zawartych w dokumentach Polityki Bezpieczeństwa, sprawdzeniu zgodności systemów z dokumentami polityki bezpieczeństwa przed dopuszczeniem systemów do przetwarzania informacji oraz uszczegółowieniu dokumentów polityki bezpieczeństwa dla grup i systemów, a także weryfikacji procedur i instrukcji.

Okresowe audyty bezpieczeństwa służą natomiast weryfikacji zgodności z założeniami polityki bezpieczeństwa systemu dla wszystkich systemów. Zalecane jest również przeprowadzanie audytu po każdej zmianie konfiguracji systemu oraz po wystąpieniu incydentu bezpieczeństwa.

Metodyka COBIT[10] (*Control Objectives for Information and Related Technology*) została opracowana przez fundację ISACF (*Information Systems Audit and*

[10] COBIT 4.1, IT Governance Institute, www.itgi.org.

Control Foundation), powołaną przez stowarzyszenie ISACA (*Information Systems Audit and Control Association*). Pierwsza publikacja metodyki COBIT nastąpiła w 1996 roku. Metodyka jest przez cały czas rozwijana. Obecnie opublikowana jest wersja 4.1.

Metodyka COBIT wskazuje warunki, jakie powinny spełniać systemy informatyczne, pozwala oceniać budowę i przebieg procesów w tych systemach. Jest jednym z narzędzi zarządzania technologią informatyczną. Ułatwia kierownictwu jednostki zrozumienie ryzyka wynikającego z funkcjonowania środowiska informatycznego.

Konieczność oceny przydatności informacji do realizacji celów biznesowych instytucji wymaga ustalenia kryteriów umożliwiających dokonanie tej oceny. Przyjęte kryteria umożliwiają ustalenie celów biznesowych i celów środowiska informatycznego.

Zasoby środowiska informatycznego zidentyfikowane w COBIT to: aplikacje, informacje, infrastruktura i ludzie.

COBIT przedstawia aktywność środowiska IT w postaci 34 procesów realizowanych w ramach czterech domen. Definiuje cele kontrolne dla wszystkich procesów oraz kontrole dla procesów i aplikacji.

3. Audyt wewnętrzny bezpieczeństwa systemów informatycznych w urzędach skarbowych

Audyt wewnętrzny w urzędach skarbowych województwa zachodniopomorskiego jest realizowany na podstawie art. 51 ust. 12 ustawy o finansach publicznych[11] przez audytorów wewnętrznych Izby Skarbowej w Szczecinie.

Potrzeba prowadzenia audytu wewnętrznego z zakresu bezpieczeństwa systemów informatycznych wynikła już w trakcie przygotowywania pierwszego planu audytu. Dokonana została analiza obszarów ryzyka, w której udział wzięli również kierownicy wszystkich jednostek[12] podległych, w których zespół audytu miał realizować audyt wewnętrzny, czyli naczelnicy urzędów skarbowych. To oni właśnie wysoko ocenili ryzyko w tym obszarze.

W związku z tym, że realizacja zadania wymaga wiedzy specjalistycznej, do każdego zadania powoływani są dwaj rzeczoznawcy, z których jeden jest informa-

[11] Ustawa o finansach publicznych...

[12] Rozporządzenie w sprawie sposobu i trybu przeprowadzania audytu..., § 6 ust. 3.

tykiem z długoletnią praktyką zarówno w tworzeniu oprogramowania, jak i administrowaniu systemami informatycznymi, a drugi jest zaawansowanym użytkownikiem. Spośród audytorów kierownik komórki audytu wewnętrznego wyznaczył audytora, który jest specjalistą z długim stażem w zakresie zabezpieczeń fizycznych. Taki skład osobowy zapewnia szerokie spojrzenie na badane zagadnienia i stwarza możliwości właściwej oceny stanu faktycznego.

Przygotowanie realizacji zadania audytowego wymaga przeanalizowania szeregu dokumentów wewnętrznych audytowanego urzędu opisujących organizację jednostki i zakresy odpowiedzialności personelu. W skład tych dokumentów wchodzą:

– regulamin organizacyjny urzędu,
– zakresy czynności pracowników realizujących zadania związane z tematem zadania audytowego,
– polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym oraz inne wewnętrzne uregulowania dotyczące zagadnień związanych z bezpieczeństwem systemów informatycznych,
– wykaz aplikacji według dostarczonego przez zespół audytowy wzoru.
– Przed zespołem audytowym postawione zostały następujące **cele zadania audytowego**:
– uzyskanie racjonalnej pewności, że systemy informatyczne są odpowiednio chronione,
– dostarczenie kierownictwu Urzędu obiektywnych analiz i ocen dotyczących badanego obszaru.
– ustalenie, czy istnieją plany działania w wypadku zaistnienia sytuacji kryzysowej.

Ważnym celem audytu, niewyszczególnionym na piśmie, jest cel edukacyjny. Dyskusje prowadzone w trakcie przeprowadzania badań i późniejszego omawiania zaleceń podwyższają świadomość pracowników jednostek audytowanych w zakresie objętym tematem zadania audytowego.

W zakresie podmiotowym zadania audytowego wskazane są komórki organizacyjne urzędu skarbowego, realizujące zadania objęte audytem. Zwykle są to komórka informatyki i komórka spraw ogólnych. Oprócz nich wskazane zostają inne komórki, w których zakresie zadań umieszczone zostały zagadnienia związane z bezpieczeństwem systemów informatycznych.

Duża różnorodność stosowanych rozwiązań występuje szczególnie w zakresie sprawowania funkcji administratora bezpieczeństwa informacji oraz w zakresie odpowiedzialności pełnomocnika ochrony informacji niejawnych za bezpieczeństwo fizyczne jednostki organizacyjnej.

Zakres przedmiotowy zadania audytowego obejmuje następujące obiekty:

- dokumentacja zabezpieczenia jednostki organizacyjnej i systemu informatycznego,
- analiza ryzyka,
- zabezpieczenia fizyczne budynków i serwerowni,
- zarządzanie uprawnieniami,
- zabezpieczanie danych w systemie informatycznym,
- nadzór nad funkcjonowaniem sieci lokalnej,
- użytkowanie notebooków,
- zasilanie urządzeń systemu informatycznego,
- zabezpieczanie danych przed działaniem szkodliwego oprogramowania,
- plany awaryjne.

Przy realizacji przedmiotowego zadania audytowego wykorzystywane są następujące metody kontrolno-badawcze:

- kwestionariusz samooceny ryzyka w zakresie zabezpieczenia systemów informatycznych,
- wywiady dokumentowane w postaci kwestionariuszy kontroli wewnętrznej (KKW) w zakresie zabezpieczenia systemów informatycznych przeprowadzane z: naczelnikiem urzędu, pracownikami komórki informatyki, pracownikami odpowiedzialnymi za bezpieczeństwo systemów informatycznych lub jednostki organizacyjnej, kierownikami aplikacji lub pracownikami odpowiedzialnymi za zarządzanie prawami dostępu,
- wizja lokalna dokumentowana w postaci listy kontrolnej,
- arkusz ustaleń audytu w pozostałym zakresie.

Zadanie audytowe na terenie urzędu realizowane jest w dwóch etapach. Powodem tego jest zamiar możliwie najmniejszego obciążenia urzędu audytem oraz minimalizacja kosztów. Pierwszy etap trwa trzy – cztery dni robocze i w tym czasie realizowane są badania, których wykonanie wymaga obecności zespołu w siedzibie urzędu.

Drugi etap trwa zwykle jeden, czasem dwa dni, i realizowany jest około dwa tygodnie po zakończeniu etapu pierwszego. W drugim etapie następuje przeprowadzenie badań uzupełniających oraz przeprowadzenie narady zamykającej i przedstawienie sprawozdania wstępnego.

Analiza ryzyka na etapie realizacji zadania audytowego odbywa się na podstawie **kwestionariusza samooceny** ryzyka. Kwestionariusze samooceny wypełniają wszyscy kierownicy komórek organizacyjnych urzędu, włączając w to koordynatorów wieloosobowych stanowisk pracy, oraz ścisłe kierownictwo urzędu – naczelnik, zastępcy naczelnika, główny księgowy.

Kadra kierownicza wskazuje obszary, w których sama dostrzega zagrożenia. W celu zapewnienia wysokiej obiektywności i nie sugerowania się wypowiedziami innych osób kwestionariusze wypełniane są jednocześnie przez wszystkie osoby podlegające badaniu zgromadzone w jednym miejscu, na przykład w sali szkoleniowej. Osoby te proszone są o nie komunikowanie się ze sobą i samodzielne wypełnianie kwestionariusza, a audytor i rzeczoznawcy w razie potrzeby wyjaśniają wątpliwości ankietowanych.

Kwestionariusz samooceny składa się z 22 pytań, na które można odpowiedzieć „Tak", „Nie", „Nie wiem" oraz ewentualnie rozszerzyć wypowiedź w rubryce „Uwagi".

Kwestionariusze wypełniane są anonimowo. Dane z kwestionariuszy wprowadzane są do przygotowanego arkusza kalkulacyjnego w celu przeprowadzenia analizy, graficznego przedstawienia wyników i wyciągnięcia wniosków. Wnioski mają wpływ na przebieg następnych badań realizowanych przez zespół audytowy, powodują zwiększenie wagi przypisanej obszarom o podwyższonym ryzyku.

Do przeprowadzenia usystematyzowanych badań w przedmiotowym zakresie audytu bezpieczeństwa systemów informatycznych przygotowane zostały arkusze **KKW**. Kwestionariusze te ulegają zmianom wraz ze zmianami zachodzącymi w stale rozwijanych i zmieniających się systemach informatycznych oraz ze zmianami wynikającymi z rosnącego doświadczenia zespołu audytowego. Przy realizacji zadań audytowych zaplanowanych na rok 2009 zawierają one 378 pytań.

Nie wszystkie pytania zadawane są wszystkim audytowanym. Pełny zestaw pytań przeznaczony jest dla pracowników komórki informatyki oraz dla administratora bezpieczeństwa informacji.

Arkusze KKW nie są wypełniane przez audytowanych, lecz przez zespół audytowy w trakcie rozmowy z osobami audytowanymi. Rozmowy odbywają się z każdym audytowanym osobno, w pomieszczeniu zapewniającym spokój i możliwość koncentracji. Wypełniany jest kwestionariusz w postaci elektronicznej. Umożliwia to wprowadzanie dowolnie długich opisów do rubryki „Uwagi".

Taki sposób prowadzenia audytu jest bardzo czasochłonny, ale umożliwia zidentyfikowanie i szczegółowe omówienie problemów, które przy wypełnianiu kwestionariusza samodzielnie przez audytowanego mogłyby zostać pominięte lub nawet ukryte.

Po zakończeniu pierwszego etapu audytu wykonywanego w badanej jednostce następuje opracowanie informacji zebranych w arkuszach KKW i zestawienie ich w „Zbiorcze zestawienie kwestionariuszy kontroli wewnętrznej" wykonane w arkuszu kalkulacyjnym.

W zbiorczym zestawieniu informacje zebrane są w postaci zestawu arkuszy zawierających miary nadawane przez zespół audytowy, odpowiedzi i uwagi osób poddanych audytowi oraz otrzymane statystyki i opisy.

Każdy członek zespołu audytowego nadaje każdemu zagadnieniu miarę wykorzystując odpowiedzi audytowanych i wiedzę zaczerpniętą przy pomocy innych narzędzi audytowych. Przyjęto pięciostopniową skalę miar:

1) stan wysokiego zagrożenia,
2) stan średniego zagrożenia,
3) stan zagrożenia,
4) słaba strona,
5) mocna strona.

Stosowana jest także miara „0" (zero) dla pytań, które nie są oceniane, gdyż zawierają tylko informację pomocniczą.

Właściwości komórek arkusza kalkulacyjnego są tak zdefiniowane, że dla mocnej strony przybierają kolor zielony, dla słabej strony kolor pomarańczowy, dla stanów zagrożenia kolor czerwony, a dla pozycji nie ocenianych kolor biały.

Po nadaniu miar wszystkim pozycjom kwestionariusza oceny zespołu audytowego zostają zestawione. Dzięki kolorowaniu komórek arkusza widoczne są od razu zarówno różnice w ocenach pomiędzy członkami zespołu, jak i potencjalne obszary występowania zjawisk niekorzystnych i zagrożeń.

Oceny członków zespołu audytowego często znacznie się różnią. W trakcie dyskusji przedstawiane są przyczyny przyjęcia ocen i miara końcowa przyjmowana jest w wyniku uzgodnienia, a nie prostego wyliczenia średniej ocen.

Ustalenia dokonane w trakcie prowadzenia badań audytowych przy pomocy omówionych narzędzi weryfikowane są poprzez przeprowadzenie **wizji lokalnej**. Wizja lokalna służy również poszukiwaniu słabych punktów zabezpieczeń, które nie mogą być zidentyfikowane w inny sposób.

Sprawozdanie z przeprowadzonego zadania przygotowywane jest w dwóch etapach. Najpierw przygotowywane jest sprawozdanie wstępne. Prezentuje ono przede wszystkim dokonane ustalenia stanu niekorzystnego i przedstawione zostaje na naradzie zamykającej.

W trakcie przedstawiania sprawozdania wstępnego odbywa się dyskusja pomiędzy członkami zespołu audytowego i pracownikami audytowanego urzędu na temat dokonanych ustaleń i proponowanych przez zespół zaleceń. Propozycje zaleceń zespół audytowy przedstawia na naradzie zamykającej ustnie.

Na podstawie ustaleń dokonanych na naradzie zamykającej zespół audytowy przygotowuje sprawozdanie ostateczne.

Przyjęcie organizacji pracy polegającej na prezentacji sprawozdania wstępnego i jego omówieniu z pracownikami jednostki audytowanej pozwala ograniczyć pisemne zgłaszanie zastrzeżeń do sprawozdania audytowego i wskutek tego zmniejsza czas trwania i koszt realizacji zadania audytowego.

Uwagi końcowe

Wynikiem realizacji zadań audytowych jest poprawa stanu bezpieczeństwa systemów informatycznych następująca po wdrożeniu zaleceń wydanych przez zespół audytowy.

Jako niezwykle ważny element traktowany jest również wzrost stanu bezpieczeństwa wynikający z realizacji celu edukacyjnego – zwiększenia świadomości pracowników i naczelników urzędów skarbowych w zakresie bezpieczeństwa. Szerokie omówienie występujących problemów i przedstawienie argumentów popierających wskazane zalecenia powoduje większe zrozumienie konieczności wprowadzenia zmian, które często powodują powstanie ograniczeń i zmniejszenia wygody pracy.

Literatura

Byczkowski M., Marciniak P., *TISM – Total Information Security Management. Dokumentacja ver. 1.4 RC1*, www.ensi.net.
COBIT 4.1, IT Governance Institute, www.itgi.org.
Forystek M., *Audyt informatyczny*. InfoAudit Sp. z o.o., Warszawa 2005.
Kifner T., *Polityka bezpieczeństwa i ochrony informacji*. Helion, Gliwice 1999.
Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*. MIKOM, Warszawa 2003.
Radziulis J., Hołubowicz W., Knapik R., *Wymagania dotyczące bezpieczeństwa informacji i baz danych zawarte w obowiązujących w Polsce aktach prawnych*. XII Konferencja PLOUG, Zakopane 2006, www.ploug.org.pl.

Akty prawne

Ustawa z dnia 30 czerwca 2005 o finansach publicznych, DzU nr 249, poz. 2104.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, DzU nr 100, poz. 1024.
Rozporządzenie Ministra Finansów z dnia 10 kwietnia 2008 roku w sprawie sposobu i trybu przeprowadzania audytu wewnętrznego, DzU nr 66, poz. 406.

THE INTERNAL AUDIT METHODS OF SAFETY OF COMPUTERIZED INFORMATION SYSTEMS ON EXAMPLE OF TAX OFFICES OF WEST POMERANIAN PROVINCE

Summary

In the article „The internal audit methods of safety of computerized information systems on example of tax offices of west pomeranian province" has been presented the methods used in practice during realization audits, in which the article's author takes part as an expert.

There was presented domains of security of computerized information systems in the article: physical security, logical security and law security. The law security is considered in two aspects: legality of software and compliance of data processing with law. There is presented a short review of known methods of audit used in the range of discussed theme, too.

Translated by Mariusz Prawicki