Zeszyty Naukowe Wydziału Informatycznych Technik Zarządzania
Wyższej Szkoły Informatyki Stosowanej i Zarządzania
„Współczesne Problemy Zarządzania"
Nr 1/2014

ZARZĄDZANIE DOSTĘPEM DO SYSTEMÓW INFORMATYCZNYCH W ORGANIZACJACH

Natalia Volodko, Mirosław Bobrowski

Wyższa Szkoła Informatyki Stosowanej i Zarządzania
Newelska 6, 01-447 Warszawa

Artykuł, oparty na pracy dyplomowej, obronionej na Wydziale Informatycznych Technik Zarządzania, dotyczy zagadnień bezpieczeństwa systemów informatycznych, poczynając od ochrony informacji i danych jako takich, środków, jakie służą temu celowi i systemowych rozwiązań, a także ich zasadniczych cech. Dokonano przeglądu zagadnień i opinii na temat ich rozwiązywania, zwracając uwagę na praktyczną stronę zapewnienia odpowiedniego poziomu bezpieczeństwa. Naturalnym komponentem systemowego podejścia w tej dziedzinie jest odpowiednie zarządzanie dostępem.

Słowa kluczowe: system informatyczny, bezpieczeństwo, dostęp

1. Wstęp

Bezpieczeństwo informacji przetwarzanych w systemach informatycznych jest elementem właściwego zarządzania, ułatwiającym realizację misji organizacji. Dziedzina ta wymaga jasno zdefiniowanego i zintegrowanego podejścia. Jest potrzebna firmie, która dąży do utrzymania konkurencyjności, płynności finansowej i zysku, dla której ważny jest wizerunek organizacji oraz przepisy prawa. Podobnie jak inne aktywa biznesowe, stanowi podstawę działalności na rynku i musi być odpowiednio chroniona. Nie są chronione wszystkie informacje we współczesnych organizacjach, a tylko te wrażliwe informacje, które mają znaczenie dla realizacji zadań stawianych przed instytucją. Prawidłowo funkcjonujący biznes nie może już obyć się bez wsparcia rozwiązań informatycznych, a jednocześnie zaawansowane rozwiązania technologiczne stwarzają nowe formy zagrożeń. Obecnie panuje słuszne przekonanie, że ten, kto posiada informację i potrafi ją należycie ochronić, przejmuje kontrolę nad rynkiem i zyskuje przewagę nad konkurencją.

Celem pracy, prezentowanej w niniejszym tekście, był projekt procesu zarządzania dostępem do systemów informatycznych w organizacji z wybranym systemem zarządzania oraz ich optymalizacja ze względu na minimalizację zagrożeń. Wskazano również współczesne zagrożenia i sposoby zapobiegania im.

W pierwszym rozdziale pracy, wprowadzającym do tematu, opisano pojęcia związane z bezpieczeństwem informacji, wyjaśniono zastosowanie odpowiednich procedur i podział odpowiedzialności. Przedstawiono analizę wybranych norm i zagadnień prawnych, związanych z bezpieczeństwem przetwarzania danych przy użyciu systemów informatycznych. Drugi rozdział pracy zawiera wprowadzenie do systemu zarządzania bezpieczeństwem informacji. Rozdział trzeci zawiera analizę wybranych aspektów zarządzania dostępem do systemów informatycznych w organizacjach. Rozdział czwarty dotyczy tematyki zagrożeń dla bezpieczeństwa danych przetwarzanych w systemach informatycznych. Rozdział piąty związany jest z projektem procesu zarządzania dostępem do systemów informatycznych w organizacji z wybranym systemem zarządzania oraz ich usprawnienie ze względu na minimalizację zagrożeń. Zakończenie zawiera podsumowanie pracy i syntetyczne wnioski.

2. Zarządzanie dostępem

Dynamiczny rozwój społeczeństwa informacyjnego powinien uświadomić przedsiębiorcy jak ważnym aspektem jest informacja, która przybiera różne formy: może być przechowywana na nośniku papierowym, elektronicznym, wypowiadana w rozmowie i, niezależnie od tego za pomocą jakich środków jest udostępniana, zawsze niesie za sobą zagrożenie nieautoryzowanego dostępu.

Dane mogą przyjmować różną postać: znaków, mowy, wykresów. Różne dane mogą przedstawiać tę samą informację. Dane są zatem pojęciem węższym od informacji, chociaż potocznie tych pojęć używamy zamiennie. Rozpatrując to zagadnienie bardziej szczegółowo dane to surowe, niepoddane analizie fakty, liczby i zdarzenia, z których można opracować informacje. Dane w systemie informatycznym to reprezentacja informacji, zapisana w pewnym obszarze pamięci komputera. Dane mogą reprezentować pojedynczą informację, na przykład imię lub nazwisko, albo zespół powiązanych ze sobą informacji, które stanowią treść komunikatu przekazywanego za pomocą danych.

Zatem: czy otacza się ochroną informacje, czy raczej dane, a może wiedzę? W kontekście przyjętej definicji należy stwierdzić, że chronić należy zarówno informację, poprzez działania na poziomie znaczeniowym, jak i dane, których interpretacja może prowadzić do pozyskania informacji. Mimo, że znaczenie obu terminów jest różne, stanowią one wspólną wartość i są zasobem organizacji.

Jednym z aspektów ochrony informacji jest ochrona tajemnic. Prawodawstwo polskie odnosi się do wielu różnych rodzajów tajemnic. Trzeba jednak zaznaczyć, że często nie definiuje ich w sposób precyzyjny. W miarę jasna jest definicja informacji niejawnych oraz danych osobowych, choć już interpretacja pojęcia zbiorów danych osobowych wzbudza liczne kontrowersje. Istnieje w tym obszarze wiele

pojęć, takich, jak na przykład: tajemnica przedsiębiorcy, tajemnica przedsiębiorstwa, tajemnica handlowa, których definicje, jeżeli w ogóle istnieją, nie są określane jednoznacznie. Taki stan rzeczy wymaga próby zebrania różnego rodzaju tajemnic prawnie chronionych i stworzenia ich systematyki. Informacje niejawne klasyfikuje się według stopnia ich ochrony na: „zastrzeżone", „poufne", „tajne" oraz „ściśle tajne".

Pracownicy, w toku wykonywania swoich służbowych obowiązków, wchodzą w posiadanie mniej lub bardziej istotnych informacji, których pracodawca wolałby nie ujawniać na zewnątrz. Takie wrażliwe informacje czasami są wyraźnie przez pracodawcę oznaczone jako poufne poprzez zastosowane środki technicznej i fizycznej ochrony. Na ich wyjątkowy charakter zazwyczaj wskazuje także intuicja i zdrowy rozsądek.

W tej dziedzinie mamy do czynienia z ewolucją technologii informatycznych. Trendy w IT zmieniają się bardzo często i systemy same niosą pewne zagrożenia wynikające z ich awaryjności i przestarzałości. Rozwój technologii, zwłaszcza informatycznych, spotęgował zagrożenie prywatności człowieka, sferą objętą szczególną ochroną są między innymi informacje niejawne, „*know how*" i dane osobowe (dane wrażliwe). Konieczność tą dostrzeżono w miarę poszerzenia zakresu danych gromadzonych o obywatelach przez różne instytucje, publiczne i prywatne.

Rozpoczęcie działalności gospodarczej pociąga za sobą upublicznienie rozmaitych informacji dotyczących przedsiębiorcy i pracowników, należy zatem zwracać szczególną uwagę na wszelkie działania związane ze zbieraniem i dalszym przetwarzaniem danych w każdym obszarze działalności firmy i na każdym poziomie jej wewnętrznej hierarchii.

Pojęcie „ochrony danych" powinniśmy utożsamiać z „bezpieczeństwem informacji" i z ryzykiem z nim związanym. Aby wdrożyć system zarządzania bezpieczeństwem informacji, można zastosować się do określonej normy, aktu prawnego oraz rozporządzenia, które precyzują zasady wdrażania procedur. Standard to pewien wzorzec zatwierdzony przez instytucję normalizacyjną, można go uznać jako zapis prawny, lub jako podany przez autorytet, lub może on zostać przyjęty nieformalnie wskutek dużego upowszechnienia.

Przyznanie certyfikatu oznacza wyłącznie tyle**,** że produkt/system został wykonany zgodnie z zaleceniami określonego standardu i może zwiększyć atrakcyjność firmy. Zakłada się, że cechy danego produktu związane z bezpieczeństwem teleinformatycznym będą na wyższym poziomie jakościowym niż wtedy, gdy z zaleceń standardów się nie korzysta.

Rozporządzenie spełnia dwie role: regulacyjną, czyli wskazanie wymagań funkcjonalnych, bezpieczeństwa oraz edukacyjną, wskazanie wprost minimalnych wymagań dla powszechnie stosowanych rozwiązań. Do wad można zaliczyć to, iż nie uwzględnia wszystkich możliwych scenariuszy zagrożeń, szybko się dezaktualizuje, zamyka możliwości stosowania rozwiązań alternatywnych wobec wymienionych w rozporządzeniu. Do zalet zaliczamy to, że podpowiada ono wprost jakościowy i ilościowy sposób wypełniania niektórych wymagań, wskazuje kluczowe minimalne wymagania, jest powszechnie nieodpłatnie dostępne.

Bezpośrednia odpowiedzialność za bezpieczeństwo danych należy do zakresu obowiązków wykonawcy konkretnego zadania, chociaż ostateczna odpowiedzialność zawsze spoczywa na zarządzie firmy lub organizacji. Tylko, jeśli zarząd/kierownictwo troszczy się o bezpieczeństwo danych to zadania w tym zakresie są traktowane poważnie.

Interdyscyplinarny charakter zarządzania bezpieczeństwem informacji wymaga od specjalistów zajmujących się tym zagadnieniem rozległej wiedzy z różnych dziedzin zarządzania, informatyki, prawa, kryminalistyki, inżynierii systemów i psychologii. Jednocześnie, wszystkie te obszary wiedzy nie mogą funkcjonować w oderwaniu od siebie, muszą tworzyć jednolity, synergiczny System Zarządzania Bezpieczeństwem Informacji (SZBI - *ISMS (ang. Information Security Management System*). Organizacja, która chce należycie zabezpieczyć swoje informacje powinna zastosować podejście systemowe, w ramach którego będzie zarządzać kompleksowo posiadanymi aktywami informacyjnymi, infrastrukturą przeznaczoną do ich przetwarzania oraz ryzykiem dotyczącym bezpieczeństwa informacji. Dlatego w normie PN-ISO/IEC 27001: 2007 zastosowano podejście procesowe w celu, ustanawiania, wdrożenia eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia SZBI.

Identyfikacja jest fundamentem wszystkich aspektów bezpieczeństwa. Użytkownicy muszą mieć jednoznaczną tożsamość, a identyfikator jest tym, co użytkownik, pragnący korzystać z zasobów, używa w celu odróżnienia się od wszystkich innych podmiotów. Bez identyfikacji nie ma podstaw do przydzielania uprawnień i utrzymania rozliczalności.

Uwierzytelnianie biometryczne wykorzystuje unikalność określonych cech fizycznych człowieka, takich jak odciski palców, mapa siatkówki, charakterystyka głosu lub twarzy. Te fizyczne właściwości lub cechy mogą być zapisane cyfrowo, jako dane biometryczne. Biometria jest jedynym sposobem bezwzględnego przekonania się, że określona osoba jest faktycznie tą, za którą się podaje. Technologie biometryczne dzieli się na dwie grupy, wykorzystujące cechy fizyczne oraz cechy behawioralne Biometria stanowi najlepszą i najwygodniejszą metodę uwierzytelniania. Jest bezpieczna, gdy odpowiednio dobiera się technologię biometryczną, wyko-

rzystuje się bezpieczne czytniki biometryczne, zapewni się odpowiedni poziom zabezpieczania systemu IT obsługującego biometrię, wdroży się odpowiednie procedury, dotyczące rejestracji, uwierzytelniania i obsługi danych biometrycznych, zapewni się odpowiedni poziom edukacji oraz najwyższy poziom bezpieczeństwa przechowywania danych biometrycznych (wzorów). W rozwiązaniach bankowych, biometria służy przede wszystkim do weryfikacji tożsamości klienta banku i uwierzytelniania transakcji. Technologiami obowiązującymi w bankowości są, między innymi: biometria naczyń krwionośnych palca (bankomaty - Japonia, Turcja, Brazylia, Oman, Polska; oddziały - Japonia, Turcja, Polska; bankowość internetowa - Polska; płatności – Turcja; kioski informacyjne – Polska; podpis elektroniczny - Polska), biometria naczyń krwionośnych dłoni (bankomaty - Japonia, Brazylia, Turcja), biometria głosowa (call centers - USA, Izrael, Chiny, Hiszpania). Odcisk palca nie przyjął się w systemach bankowych ze względu na stosunkowo łatwą możliwość dokonywania oszustw, łatwą przechwytywalność danej biometrycznej (pozostawianie odcisków). Zniszczenie lub zabrudzenie naskórka powoduje dużą liczbę fałszywych odrzuceń. Biometria tego rodzaju jest jednak kontrowersyjna prawnie (interpretacja prawna biometrii odcisku palca może być inna niż innych biometrii). Sposób zastosowania przez administrację publiczną i policję negatywnie wpływa także na wykorzystanie w bankowości i jest to również metoda niehigieniczna.

Proponuję przyjęcie definicji „*zagrożenia*", jako potencjalnego działania człowieka lub sił wyższych, dotyczącego bezpośrednio zasobu teleinformatycznego lub organizacji procesu przetwarzania informacji i mogącego spowodować, w zależności od konkretnego atrybutu bezpieczeństwa: utratę tajności, dostępności lub integralności. Ryzyko bezpieczeństwa informacji można zdefiniować, jako prawdopodobieństwo wystąpienia zagrożenia i powstania szkód lub zniszczeń w zasobach systemu oraz przerw lub zakłóceń w jego prawidłowym funkcjonowaniu.

Ryzyko można zmniejszać, ale nigdy całkowicie nie da się go wyeliminować. Na pewnym poziomie dodawanie nowych zabezpieczeń jest znacznie kosztowniejsze niż wzrost wartości bezpieczeństwa, które przy ich pomocy można osiągnąć. Uniwersalna zasada mówi, że ryzyko należy obniżać do poziomu, w którym organizacja będzie zdolna ponieść ciężar strat spowodowanych przez zrealizowane zagrożenia i kontynuować swoją działalność.

Najpierw należy określić, co, dlaczego i jak chronić, gdyż, w największym uproszczeniu, do tego sprowadza się proces analizy zagrożeń. Jak jest w praktyce? Bardzo często organizacje nie wiedzą nawet, że należy przeprowadzić taką analizę, nie mówiąc o wykorzystaniu jej wyników. Prawie zawsze efektem jest słaba, pełna luk i niekompletna ochrona. Brak inwentaryzacji zasobów informacyjnych często prowadzi do tego, że część wrażliwych aktywów informacyjnych pozostaje niechroniona. Brak jest wiedzy o obecnych i potencjalnych zagrożeniach, która jest podsta-

wą analizy (efektem jest słabe przygotowanie na wypadek naruszenia bezpieczeństwa informacji). Brak także wiedzy o rzeczywistych skutkach, możliwych stratach w przypadku naruszenia bezpieczeństwa informacji (często dopiero analiza zagrożeń pokazuje, że pewne straty są nie do zaakceptowania i organizacja musi im zapobiegać). Nierzadki jest niewłaściwy dobór zabezpieczeń, zbyt rygorystyczna lub zbyt liberalna ochrona informacji (efektem jest występowanie ewidentnych luk w zabezpieczeniach lub brak tych zabezpieczeń; innym efektem są zabezpieczenia zbyt rygorystyczne nieadekwatne do stopnia zagrożenia), lub wybór bardzo drogich rozwiązań (np. kaskadowych haseł lub skomplikowanych i niepraktycznych procedur postępowania).

Należy pamiętać o zależności pomiędzy poziomem bezpieczeństwa systemów informatycznych, a nakładami, które trzeba ponieść. Trzeba się liczyć z kosztami, dlatego przyjęto poziomy bezpieczeństwa, wśród których maksymalny jest potrzebny, gdy niepoprawna praca systemów informatycznych prowadzi do całkowitego załamania instytucji lub wywiera szerokie niekorzystne skutki społeczne bądź gospodarcze. Niski natomiast powinien być stosowany, gdy niepoprawna praca systemów informatycznych przynosi firmie tylko niewielkie szkody.

Dla większości kadr kierowniczych firm konieczność ochrony informacji nie istnieje lub jest bardzo niewielka. Sytuacja zmienia się, gdy nastąpi ograniczenie dostępu do informacji lub utrata informacji. Gdy się to przydarzy, wiąże się często z ogromnymi kosztami finansowymi i wizerunkowymi, co dowodzi, że taniej jest zapobiegać niż „leczyć".

Nasilenie działań przestępczych, skierowanych na kradzież i nielegalne wykorzystanie informacji w sieciach telekomunikacyjnych, systematycznie wzrasta, tak jak wzrasta liczba dostępnych usług i wielkość zgromadzonych w sieci zasobów informacyjnych. Najpoważniejsze z zagrożeń to ataki hakerów, programistów posiadających szeroką wiedzę informatyczną, którzy wykorzystują luki w oprogramowaniu i bezpieczeństwie systemów informatycznych. Należą tutaj także ataki przestępców komputerowych, zwanych crackerami, którzy do celów przestępczych wykorzystują wiedzę i procedury opublikowane przez hakerów oraz nieświadomość i naiwność użytkowników.

Odrębna kategoria zagrożeń wynika z nieświadomości użytkowników i nieprzestrzegania przez nich zaleceń dotyczących bezpiecznego korzystania z systemów informatycznych. Skutkuje to podatnością na wykonywanie zagrażających bezpieczeństwu operacji, do czego użytkownik może być nakłaniany poprzez pocztę elektroniczną, zamieszczenie linków na stronach internetowych lub inne formy komunikacji, takie jak komunikatory internetowe, czy portale społecznościowe.

Wraz z postępującą "wirtualizacją" gospodarki i rozwojem e-biznesu, pojawia się coraz więcej sposobów dokonywania kradzieży tożsamości, a co za tym idzie - wzrasta zapotrzebowanie na dane osobowe. Zwiększa się również wartość innych typów poufnych danych. Znając potencjalne kanały wycieku danych, niezwykle ważne jest rozwinięcie organizacyjnych środków bezpieczeństwa oraz środków opartych na oprogramowaniu, gdyż ich wartość będzie rosła.

Nawet, jeśli nie będzie się zwalczać wewnętrznych złodziei i skupiać się całkowicie na zapobieganiu przypadkowych wycieków danych, można zmniejszyć całkowitą liczbę wycieków o trzy czwarte, co znacznie obniża koszty. Samo zapobieganie przypadkowym wyciekom pozwala zaoszczędzić znaczną sumę pieniędzy, co jest wystarczającym powodem zintegrowania systemu zapobiegania.

Ataki ukierunkowane są bardzo trudne do wykrycia i sklasyfikowania. Najistotniejszymi czynnikami w zwalczaniu tego typu ataków jest poziom świadomości użytkownika oraz wiedza personelu firm z branży bezpieczeństwa IT. Użytkownik powinien rozumieć konieczność ochrony antywirusowej, nawet jeśli nieznacznie wpływa ona na prędkość przetwarzania, w przeciwnym razie wszelkie próby stworzenia skutecznej linii obrony przed atakami ukierunkowanymi są skazane na klęskę. Innym istotnym czynnikiem jest rozwijanie proaktywnych technologii przez producentów systemów bezpieczeństwa IT.

W 2012 roku w Polsce więcej niż 7 milionów osób zetknęło się z cyberprzestępczością, na świecie ponad 550 milionów. W efekcie, każdy atak hakerów naraża firmy na straty rzędu 100-300 tys. USD. To najnowsze dane, opublikowane przez Check Point Software Technologies w raporcie Security Report 2013. Badanie pokazuje, że co 23 minuty użytkownicy komputerów stają się ofiarami ataków, wchodząc na zainfekowane strony w Internecie. Ponad 50 % badanych firm miała zainfekowane wewnętrzne sieci, z których pracownicy pobierali dane. Przez ostatnie dwa lata liczba ataków, zakończonych kradzieżą danych, znacznie wzrosła. Ich ofiarą padali wszyscy: amerykańskie i europejskie instytucje rządowe, firmy zbrojeniowe, największe korporacje, a nawet organizacje praw człowieka. Według badań, 75% przedsiębiorstw przyznało, że było ofiarą ataków hakerów, a włamania prowadzą do zakłócenia funkcjonowania firmy oraz utraty poufnych informacji, w tym własności intelektualnej oraz sekretów handlowych.

Media regularnie informują o nowych atakach i wyciekach danych najczęściej osobowych, dotyczą one nie tylko wielkich firm czy korporacji typu Google, Sony i instytucji państwowych, ale i szkół, banków, małych instytucji. Jedną z częstszych przyczyn zaistnienia zagrożenia bezpieczeństwa jest niewłaściwe, często nieświadome, działanie pracownika.

Mimo dynamicznej informatyzacji oraz rozwoju społeczności informacyjnej, wzrost budżetów przeznaczanych na bezpieczeństwo wielu firm w obszarze IT jest znikomy. Dzieje się tak przede wszystkim dlatego, że oszacowanie korzyści, jakie niosą ze sobą inwestycje w bezpieczeństwo informacji jest niezwykle trudne.

Człowiek jest najsłabszym ogniwem w systemie bezpieczeństwa informacji. Łatwo sobie wyobrazić sytuację, w której jeden z pracowników firmy przez swoją niedbałość w wykonywaniu obowiązków naraził organizację na szkody spowodowane utratą lub zniszczeniem danych. Albo pokusił się o udostępnienie konkurencji chronionych danych w zamian za korzyści finansowe lub inne profity. Niestety, sytuacje tego typu zdarzają się coraz częściej, a wynikają również z braku wdrożonego systemu bezpieczeństwa informacji i są konsekwencją braku szkoleń uświadamiających wśród pracowników.

Szkolenia użytkowników, dotyczące wdrożonego systemu bezpieczeństwa informacji są jednym z ważniejszych elementów jego działania. Użytkownicy muszą być świadomi, reagować i działać na zagrożenia. Powinni właściwie posługiwać i postępować z urządzeniami przetwarzającymi informacje, by zminimalizować ryzyko jej utraty. Wszyscy pracownicy powinni przejść właściwe, okresowo uaktualniane, przeszkolenie w zakresie polityki i procedur organizacji, a ich kwalifikacje w tym zakresie powinny być stale podnoszone. Elementem niezbędnym w trakcie zatrudniania nowego pracownika jest przedstawienie mu stosownej umowy o zachowaniu poufności i o tajemnicy firmowej, stanowiącej część majątku organizacji.

Zarządzanie prawami dostępu personelu jest konieczne w celu ograniczenia możliwości ujawnienia poufnych informacji. Obowiązywać ma zasada minimalnych przywilejów, prawa dostępu przypisywane użytkownikom muszą stanowić niezbędne minimum konieczne im do wykonywania swoich obowiązków. Wszelkie prośby o zmiany, których rezultatem jest rozszerzenie praw dostępu muszą być uwzględniane zgodnie z instrukcją zarządzania dostępem do zasobów IT. Zwierzchnik pracownika powinien mieć obowiązek zwracania się do departamentu bezpieczeństwa z prośbą o nowe uprawnienia, dopiero po analizie i akceptacji taki dostęp powinien być nadany przez IT.

Zarządzanie incydentami wspiera analizę ryzyka, gdyż weryfikuje w praktyce uzyskane w jej toku wyniki szacunkowe i ułatwia przy tym ich wykorzystanie przy wprowadzaniu niezbędnych udoskonaleń. Wnioski z analizy incydentów powinny znaleźć odzwierciedlenie w programach uświadamiających i szkoleniowych. Doskonałym materiałem szkoleniowym mogą być studia przypadków incydentów, niekoniecznie zarejestrowanych we własnej instytucji, ale istotnych ze względu na możliwe analogie. Proces zarządzania incydentami stanowi główne źródło informacji o efektywności systemu bezpieczeństwa. Informacje te są gromadzone, podda-

wane analizom porównawczym w ustalonych przedziałach czasowych, a także śledzone są trendy występowania różnego rodzaju incydentów oraz ich skutki. Na tej podstawie są wypracowane decyzje korygujące. Porównywanie zjawisk prawdopodobnych (analiza ryzyka) z tymi, które rzeczywiście miały miejsce (analiza incydentów), pozwala urealnić proces analizy ryzyka, podnieść efektywność zarządzania bezpieczeństwem, a przez to uszczelnić system bezpieczeństwa instytucji.

Dla przedsiębiorców kwestią priorytetową staje się więc budowanie odpowiedniej świadomości swoich pracowników oraz zapewnienie efektywności procedur związanych z wykorzystaniem komputera służbowego, zgodnie z jego przeznaczeniem. Pracownicy powinni mieć świadomość, że bezpieczeństwo informatyczne firmy, w której pracują, w znacznym stopniu zależy właśnie od nich.

3. Zakończenie

W zakończeniu pracy przedstawiono wnioski z analizy zarządzania dostępem do systemów informatycznych w wybranej organizacji. Dołączono także zalecenia dla budowy informatycznych systemów zarządzania w organizacjach w zakresie aspektów, które nie zostały omówione w pracy ze względu na jej ograniczoną objętość.

Należy znaleźć rozsądny kompromis między bezpieczeństwem i wydajnością pracy. Chronić należy zarówno informację poprzez działania na poziomie znaczeniowym, jak i dane, których interpretacja może prowadzić do pozyskania informacji.

Utrata lub udostępnianie informacji, które stanowią tajemnicę, bądź własność intelektualną, lub handlową, należącą do organizacji, może wywołać kłopoty natury prawnej, a nawet oznaczać utratę reputacji i zakończenie działalności. Z tego względu informację trzeba należycie chronić oraz odpowiednio nią zarządzać.

Zarządzanie dostępem jest ogółem skoordynowanych działań kierowania i zarządzania organizacją z uwzględnieniem bezpiecznego dostępu, podejmowanych w celu osiągnięcia wcześniej sformułowanych założeń. Jest elementem właściwego zarządzania, ułatwiającym realizację misji organizacji. Przedsiębiorca powinien dostrzec, że dziedzina ta wymaga jasno zdefiniowanego i zintegrowanego podejścia. Odpowiedzialność oraz zasady rozliczania użytkowników powinny być jednoznaczne, a skuteczność zabezpieczeń okresowo weryfikowana.

Zapewnienie bezpieczeństwa informacji nie jest działaniem jednorazowym, lecz jest złożonym procesem, w którego sprawne funkcjonowanie powinni się włączyć wszyscy pracownicy, kierownictwo, a także inne osoby bądź firmy współpracujące z daną organizacją. Tworzenie polityki musi być realizowane wspólnym wy-

siłkiem personelu technicznego i decydentów. Personel techniczny jest w stanie ocenić skutki różnych wariantów polityki oraz jej implementację. Decydenci są w stanie wymusić wprowadzenie polityki w życie. Polityka, której nie można zaimplementować lub wdrożyć, jest nieużyteczna. Tworzenie jej ściśle według funkcjonujących już standardów jest błędem, ponieważ pomiędzy organizacjami istnieją duże różnice. Należy, więc pamiętać o występujących różnicach w zakresie wymagań i potrzeb.

Każdy system jest tak bezpieczny jak jego najsłabsze ogniwo, czyli przede wszystkim człowiek. Od jego wiedzy, dyscypliny, odpowiedzialności i uczciwości zależy, czy poniesiemy straty natury finansowej bądź reputacyjnej. Konieczne jest kompleksowe myślenie i wdrażanie zarządzania bezpieczeństwem oraz zaangażowanie wszystkich pracowników, a szczególnie znajomość tej problematyki przez ścisłą kadrę kierowniczą. Jedną z częstszych przyczyn zaistnienia zagrożenia bezpieczeństwa jest niewłaściwe, często nieświadome, działanie pracownika.

Dla przedsiębiorców kwestią priorytetową staje się, więc budowanie odpowiedniej świadomości swoich pracowników oraz zapewnienie efektywności procedur związanych z wykorzystaniem komputera służbowego, zgodnie z jego przeznaczeniem. Pracownicy powinni mieć świadomość, że bezpieczeństwo informatyczne firmy, w której pracują, w znacznym stopniu zależy właśnie od nich.

W Polsce wciąż panuje stereotypowe myślenie o bezpieczeństwie informacji, widzianym przez pryzmat ochrony informacji niejawnych, czy też ustawowego obowiązku ochrony danych osobowych. Powoduje to, że nie są analizowane rzeczywiste zagrożenia i rezultaty utraty informacji.

Analizując okres ostatnich zmian można wywnioskować, że prawo nie ma szans nadążyć za przemianami społecznymi i gospodarczymi, wymuszanymi postępem informatyzacji. Efekt jest taki, że kiedy już uchwali się nowe prawo, najczęściej zderza się ono z nową rzeczywistością techniczną i wykreowaną społeczną, do obsługi której nie jest dostosowane. Skutki braku nadążania prawa można zminimalizować poprzez właściwe zarządzanie bezpieczeństwem informacji i dobre zdefiniowanie polityki bezpieczeństwa informacji.

Możliwe jest łączenie metodyk sterowania dostępem w celu osiągnięcia wyższego poziomu ochrony systemu. Takie połączenie jest proste i naturalne tylko w przypadku, gdy nie występują konflikty polegające na tym, że jedna z metodyk stwierdza, iż określony dostęp jest uprawniony, podczas, gdy inna zabrania dostępu. Konflikty te można rozwiązać na poziomie definiowania polityki bezpieczeństwa lub zmian organizacyjnych.

Biometria będzie jedynym sposobem bezwzględnego przekonania się, że określona osoba jest faktycznie tą, za którą się podaje. Jest ona efektywna, gdy odpowiednio dobiera się technologię biometryczną według wyznaczonych kryteriów oraz zapewnia się odpowiedni poziom zabezpieczania systemu IT. Ponadto, gdy zapewni się odpowiedni poziom edukacji i najwyższy poziom bezpieczeństwa przechowywania danych biometrycznych (wzorów). Biometria jest potrzebna, gdyż stanowi obecnie najlepszą i najwygodniejszą metodę uwierzytelniania.

Zarządzanie zabezpieczaniem systemu informatycznego to długotrwały i dynamiczny proces. Zbyt szybkie i restrykcyjne wdrażanie bezpieczeństwa systemu deprecjonuje jego wartość i rodzi nowe zagrożenia. Wdrażając system zabezpieczeń trzeba wyeliminować przesadę, a szczególnie - przekonanie o możliwości osiągnięcia absolutnego bezpieczeństwa. Powinniśmy dopasować zabezpieczenia na profilu działalności oraz pamiętać żadne nie jest absolutnie pewne.

Bibliografia

Książki:

Anderson, R. (2002) *Inżynieria Zabezpieczeń,* Wydawnictwo Naukowo Techniczne, Warszawa.

Białas, A. (2006, 2007) *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie,* Wydawnictwo Naukowo-Techniczne, Warszawa.

Kaczmarek, A. (2007) *ABC Bezpieczeństwa Danych Osobowych Przetwarzanych przy Użyciu Systemów Informatycznych,* Wydawnictwo Sejmowe, Warszawa.

Kaczmarek, A. (2009) *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych,* GIODO, Warszawa.

Kowalik, A. (2007) *ABC Ochrony Danych Osobowych,* Wydawnictwo Sejmowe, Warszawa.

Liderman, K. (2009) *Analiza Ryzyka i Ochrona Informacji w Systemach Komputerowych,* W. N. PWN, Warszawa.

Liderman, K. (2001) *Bezpieczeństwo Informacji w Systemach Informatycznych*, WSISiZ, Warszawa.

Mitnick, K. (2003) *Sztuka Podstępu,* Helion, Gliwice.

Molski M., Opala S. (2002) *Elementarz Bezpieczeństwa Systemów Informatycznych*, Mikom, Warszawa.

Pipkin, D. L. (2002) *Bezpieczeństwo informacji, ochrona globalnego przedsiębiorstwa,* Wydawnictwo Naukowo Techniczne, Warszawa.

Polaczek, T. (2006) *Audyt Bezpieczeństwa Informacji w Praktyce,* Helion, Gliwice.

Stokłosa, J., Bilski, T., Pankowski, T. (2001) *Bezpieczeństwo danych w systemach informatycznych,* W. N. PWN, Warszawa- Poznań.

Normy:

PN-EN ISO 9001 *Systemy zarządzania jakością – Wymagania,* PKN *(wersja Polska)* 2009;
PN-ISO 31000 *Zarządzanie ryzykiem- Zasady i wytyczne,* PKN, Warszawa 2012.

PN-ISO/IEC 17799:2005 *Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji.* PKN 2007;
PN-ISO/IEC 27001 *Technika informatyczna- Techniki bezpieczeństwa- Systemy zarządzania bezpieczeństwem informacji- Wymagania,* PKN, Warszawa 2007;

Rozporządzenia:

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji, Dz. U. Nr 100 z dn. 1 maja 2004 r., *z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.*

Ustawy:

Ustawa z dnia 29 października 2010 r. o zmianie ustawy o ochronie danych osobowych oraz niektórych innych ustaw (Dz. U. z 2010 r., Nr 229, poz. 1497);
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.);
Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., nr 88, poz. 553 z późn. zm.).

Artykuły:

Blim M., *Normalizacja w zarządzaniu bezpieczeństwem-nowe spojrzenie,* Zabezpieczenia 4/2009, str. 46-52;
Check Point 2013 Security Report, www.checkpoint.com;
Materiały dydaktyczne przygotowane w ramach projektu „*Opracowanie programów nauczania na odległość na kierunku studiów wyższych – Informatyka*" http://wazniak.mimuw.edu.pl;
Namiestnikow J., - Ekspert z Kaspersky Lab, *Zagrożenia w drugim kwartale 2010* (statystyki) artykuł ze strony www.money.pl ;
Polski glosariusz ITIL, wersja 3.0, www.itil-officialsite.com;
Portal Zarządzania IT, http://itsm.itlife.pl;
Raport Deloitte i Gazeta.pl*, Bezpieczeństwo ma znaczenie*: Polska edycja badania na temat bezpieczeństwa informacji w Internecie, 2009;
Sierota K., *Studium audytów bezpieczeństwa informacji, czyli nieprawidłowości w ochronie informacji. Część II,* Zabezpieczenia 4/2010.str 24-25;
Usługa Active Directory, http://technet.microsoft.com;
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001 Cz. 1. Wprowadzenie,* Zabezpieczenia 2/2008, str. 68-73;
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001 Cz. 2. Procesy zarządzania Bezpieczeństwem informacji,* Zabezpieczenia 3/4/2008, str. 74-77;
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001 Cz. 3. Elementy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),* Zabezpieczenia 5/2008, str. 26-28;
Wójcik A., *System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/IEC 27001 Cz. 4. Model PDCA w procesach SZBI (ISMS),* Zabezpieczenia 6/2008, str. 69-74;
Wyścig zbrojeń hakerów trwa, www.pcworld.pl;
Zarządzanie uprawnieniami dostępu (ITIL), www.governica.com.

Praca naukowa:

Siemkowicz P. *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym - z uwzględnieniem aktualnych zmian nowelizacyjnych,* Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Wydział Prawa, Administracji i Ekonomii Uniwersytet Wrocławski Opublikowane: 26 listopada 2009 r. e-biuletyn 2/2009.

Konferencje:

Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym, 21.03.2011 r.

Zabezpieczenie danych osobowych - aktualny stan prawny a rzeczywiste potrzeby, 28.03.2011 r.

Adamczyk A., *Klasyfikacja informacji i danych prawnie chronionych oraz wymagania dotyczące środków informatycznych przeznaczonych do ich przechowywania i przetwarzania*, www.ploug.org.pl.

Pejaś J., *Modele Kontroli Dostępu*, Politechnika Szczecińska, Wydział Informatyki.

Jakubiak P., *Rola administratora w polityce bezpieczeństwa informacji*.

Wojciechowska-Filipek S., *Metody Kontroli Dostępu w Bankowości Elektronicznej,* www.ptzp.org.pl.

Woszczyński T., *Bezpieczeństwo systemów biometrycznych na przykładzie biometrii naczyń krwionośnych palca*, www.ncpi.org.pl.

Bezpieczeństwo i Niezawodność Systemów Informatycznych, 20.09.2011 r.

Reforma Ochrony Prywatności, 16.12.2010 r.

Bezpieczeństwo IT, 6.04.2011 r.