PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1144 — 2006
Informatyka Ekonomiczna 9

Leszek Ziora

WYBRANE ASPEKTY BEZPIECZEŃSTWA DANYCH W SYSTEMACH INFORMATYCZNYCH

1. Wstęp

Obecnie trudno jest sobie wyobrazić organizację, która funkcjonowałaby bez wykorzystania systemów informatycznych. W każdym przedsiębiorstwie znajdują się informacje dotyczące poszczególnych szczebli zarządzania strategicznego, taktycznego i operacyjnego [Nowicki 2002]. Informacje te z racji swojej ważności powinny być odpowiednio zabezpieczone. Dopuszczenie do naruszenia bezpieczeństwa systemów informatycznych przedsiębiorstwa powoduje nie tylko bezpośrednie straty finansowe, ale również zmniejszenie sprzedaży i możliwości konkurowania, podważenie wiarygodności, utratę dobrej marki, utratę zaufania klienta, niemożność prowadzenia działalności, narażenie się na kosztowne procesy prawne na skutek udostępnienia prywatnych i poufnych informacji [Nowicki, Unold 2002]. Podstawą bezpiecznego działania systemu informatycznego w przedsiębiorstwie powinien być formalny dokument zwany polityką bezpieczeństwa, opisujący reguły tworzenia i użytkowania bezpiecznego systemu [Nowicki, Ziora, Rot 2005].

2. Istota bezpieczeństwa danych

Przez pojęcie bezpieczeństwa danych należy rozumieć ogół środków i procedur mających na celu niedopuszczenie do zniszczenia, utraty, kopiowania, modyfikacji lub zdradzenia treści informacji przez osoby fizyczne lub prawne [Nowicki 2002].

Zniszczenie ma miejsce wtedy, gdy nośnik informacji ulegnie uszkodzeniu i zostanie pozbawiony wartości użytkowych. W takim wypadku niemożliwe staje się odczytanie informacji, a co z tego wynika – skorzystanie z nich. Przez kradzież informacji rozumie się z kolei jej przechwycenie przez intruza. Staje się on wtedy jej użytkownikiem, pozbawiając właściciela możliwości skorzystania z niej.

Modyfikacja polega na nieautoryzowanym dokonaniu zmian treści informacji. Działanie to powoduje to, iż informacja staje się bezużyteczna, a w przypadku niezdawania sobie sprawy przez właściciela z faktu korzystania ze zmodyfikowanej informacji może okazać się szkodliwa.

Kopiowanie to powielenie informacji przez intruza bez ingerencji w jej treść. W porównaniu z wykonaniem kopii na nośnikach tradycyjnych na powielenie informacji na nośniku elektronicznym intruz potrzebuje stosunkowo krótkiego czasu.

Zdradzenie treści polega na dotarciu intruza do dokumentu i zapamiętaniu go. W tym przypadku nie zostaje dokonana żadna ingerencja. W dokumentacji papierowej nie są potrzebne żadne środki techniczne, w dokumentacji zapisanej na nośniku komputerowym zaś konieczne jest skorzystanie przez osobę niepowołaną ze sprzętu właściciela. Taki rodzaj ataku wykorzystywany jest szczególnie w przypadku krótkich informacji o dużej tajności [Nowicki 2002].

Oprócz pojęcia bezpieczeństwa istnieją definicje środków bezpieczeństwa, poufności, tajności oraz nienaruszalności, czyli integralności danych [Molski, Opala 2002].

- środki bezpieczeństwa to zabezpieczenia technologiczne i środki administracyjne, które można zastosować do komputerów, programów i danych w celu zapewnienia ochrony interesów przedsiębiorstw oraz poufności indywidualnej;
- tajność to atrybut danych opisujących stopień ochrony, jakiej dane mogą podlegać, uzgodniony przez osoby lub organizacje otrzymujące te dane;
- poufność to prawo jednostki do decydowania o tym, jakimi informacjami chce się podzielić z innymi ludźmi i jakie informacje jest skłonna od nich przyjąć – z pojęciem tym wiąże się szyfrowanie;
- nienaruszalność danych to cecha określająca, że dane nie różnią się od danych źródłowych i nie zostały przypadkowo lub umyślnie zmodyfikowane, ujawnione lub zniszczone.

Istotny wpływ na nienaruszalność danych mają: systemy operacyjne, które to klasyfikuje pomarańczowa księga oraz jej rozszerzenie ITSEC, systemy uwierzytelniania i autoryzacji oraz urządzenia biometryczne, fizyczna kontrola dostępu do obiektów systemu, tzn. zabezpieczone szafy rackowe, kamery monitorujące, czytniki kart, ochrona antywirusowa oraz sprzętowe i programowe zapory sieciowe (firewale). Bezpieczeństwo systemu informacyjnego polega na zapewnieniu dostępności systemu oraz nienaruszalności poufności informacji przetwarzanych przez ten system. W ramach dostępności należy zagwarantować sprawne działanie wszystkich jego elementów. Związane z tym są takie działania, jak [Nowicki, Unold 2002]: ochrona przed utratą zasilania i przed przepięciami, ochrona przed awarią pamięci dyskowej, archiwizacja danych – pamięci taśmowe, CD, CD RW, DVD, DVD RW itp., ochrona przed uszkodzeniami jednostki centralnej, ochrona przed niesprawnością sieci komputerowej – stosowanie połączeń redundantnych, dublowanie urządzeń sieciowych, zapewnienie połączenia do i z sieci Internet, (także z wykorzystaniem cache, proxy), zarządzanie inwentaryzacją sprzętu informatycznego.

3. Międzynarodowe standardy klas bezpieczeństwa

W celu określenia klas lub inaczej poziomów bezpieczeństwa w sposób zunifikowany zostały opracowane ujednolicone kryteria bezpieczeństwa systemów informatycznych. W dokumencie Trusted Computer Standards Evaluation Criteria, znanym także jako Orange Book, Departament Obrony USA zdefiniował siedem poziomów bezpieczeństwa komputerowego systemu operacyjnego. Różne poziomy określają różne sposoby zabezpieczania sprzętu, oprogramowania i danych. Klasyfikacja ma charakter „zawierania", co oznacza, że wyższe poziomy mają wszystkie cechy poziomów niższych [Scambray, McClure, Kurtz 2001].

D1 – najniższy poziom bezpieczeństwa określający także całkowity brak wiarygodności systemu. Poziom ten nie wymaga certyfikacji, oznacza on brak jakichkolwiek zabezpieczeń.

C1 – na tym poziomie system operacyjny kontroluje uprawnienia użytkowników do odczytu i zapisu plików i kartotek oraz dysponuje mechanizmem autoryzacji dostępu. System taki nie ma na ogół zdefiniowanego tzw. superużytkownika (np. w UNIX root) lub użytkownik taki nie jest bardziej „bezpieczny" niż pozostali. Poziom C1 jest także pozbawiony mechanizmów rejestrowania zdarzeń.

C2 – poziom ten gwarantuje automatyczne rejestrowanie wszystkich istotnych z punktu widzenia bezpieczeństwa zdarzeń i zapewnia silniejszą ochronę głównych danych systemowych, takich jak np. baza danych haseł użytkowych.

B1 – klasa ta obsługuje bezpieczeństwo na kilku poziomach, takich jak „tajne" i „ściśle tajne". Ma wdrożone mechanizmy uznaniowej kontroli dostępu do zasobów systemu, co może np. sprowadzić się do braku możliwości zmiany charakterystyki dostępu do plików i kartotek przez określonego użytkownika.

B2 – poziom ten wymaga przypisania każdemu obiektowi systemu komputerowego etykiety bezpieczeństwa określającej status tego obiektu w odniesieniu do przyjętej polityki bezpieczeństwa. Etykiety te mogą zmieniać się dynamicznie w zależności od tego, co jest aktualnie użytkowane.

B3 – jest to rozszerzenie problemu bezpieczeństwa na sprzęt komputerowy. W tym przypadku bezwzględnie obowiązkowe jest chronienie zarówno przechowywanej, jak i przesyłanej informacji.

A1 – jest to najwyższy poziom bezpieczeństwa. Cała konfiguracja sprzętowo-programowa wymaga matematycznej weryfikacji. Zarówno sprzęt, jak i oprogramowanie musi podlegać specjalnej ochronie w trakcie transportu zapewniającej jego nienaruszalność.

W Europie prace nad ustaleniem międzynarodowych kryteriów oceny bezpieczeństwa systemów informatycznych rozpoczęto pod koniec lat osiemdziesiątych. W 1991 r. eksperci z Francji, Niemiec, Holandii i Wielkiej Brytanii ogłosili kryteria oceny bezpieczeństwa technologii informacyjnej (*information technology security evaluation criteria* – ITSEC). ITSEC stanowi próbę poszerzenia „pomarańczowej księgi". W porównaniu z nią w ITSEC funkcjonalność systemu dodatkowo nacechowana jest takimi ocenami, jak: wierność obejmująca wykrywanie i prewencję,

niezawodność pracy, gwarantującą dostęp do zasobów systemu w wymaganym czasie, wymianę danych, usługi związane z zabezpieczeniem kanałów transmisyjnych. ITSEC definiuje siedem klas pewności od poziomu E0 do E6. Podobnie jak w „pomarańczowej księdze" na każdy wyższy poziom składają się wymagania niższego poziomu.

4. Klasyfikacja zagrożeń systemów informatycznych

Każdy system informatyczny narażony jest na różnorodne zagrożenia. Mogą one mieć charakter elektroniczny i fizyczny. Te pierwsze występują ze strony hakerów i intruzów, którzy atakują strony internetowe, systemy poczty elektronicznej lub wewnętrzne oprogramowanie firm. Zagrożenia fizyczne są powodowane przez nieuczciwych administratorów sieci, pracowników i kontrahentów, mogą je również wywoływać pożary, ładunki wybuchowe, powodzie. Przyczyny te mogą mieć charakter losowy bądź też być celowym działaniem [Grzywacz 2003].

Zagrożenie o charakterze elektronicznym można nazwać agresją elektroniczną, która polega na uzyskaniu przez intruza dostępu do komputera będącego częścią sieci przedsiębiorstwa albo śledzeniu danych przepływających przez sieć. Do typowych zagrożeń systemów informatycznych można zaliczyć [Niezgódka 1999]:

- ataki z zewnątrz, w tym narzędzia powodujące blokadę usług sieciowych (ataki typu DOS – *denial of service*),
- wirusy, robaki internetowe, bomby poczty elektronicznej oraz konie trojańskie,
- niezadowolony lub nieuczciwy personel,
- problemy fizyczne, takie jak awarie, katastrofy,
- pomyłki ludzi.

Ataki z zewnątrz typu **DoS** mogą tymczasowo unieruchomić całą sieć. Celem blokady usług jest pozbawienie użytkowników możliwości korzystania z usług sieciowych – od zajęcia całego pasma, po wymuszenie załamania serwera. Każde takie działanie jest w świetle prawa nielegalne i dokonywane we wrogich zamiarach. Atak polegający na blokowaniu usług wykorzystuje właściwości protokołu IP, zatem może być wyprowadzony przeciw serwerowi na dowolnej platformie systemowej.

Programy destrukcyjne mają na celu nękanie użytkowników i/lub niszczenie danych. Można do nich zaliczyć wirusy, robaki internetowe, konie trojańskie. Wirus komputerowy jest programem przyłączającym się do plików na komputerze, który atakuje. Wówczas oryginalny kod wirusa zostaje dopisany do zawartości niektórych plików w systemie. Proces ten nazywamy infekcją. Zainfekowany plik staje się nosicielem i sam może infekować inne pliki. Jest to replikacja. Poprzez proces replikacji wirus rozprzestrzenia się po całym dysku twardym, doprowadzając do infekcji całego systemu. Często oznaki tego procesu są niezauważalne do czasu aż nastąpi infekcja całego systemu. Do podstawowych działań wirusów należą [Grzywacz 2003]: blokowanie działania komputera przez uszkodzenie

systemu operacyjnego, niszczenie danych znajdujących się na dyskach zainfekowanych komputerów, celowe spowolnienie działania komputera uniemożliwiające jego wykorzystanie, wyświetlanie obrazów, haseł ideologicznych, odwracanie obrazu na ekranie monitora, zamiana klawiszy myszy i inne podobne działania mające charakter dowcipu, wykradanie informacji ważnych w aspekcie bezpieczeństwa sieci komputerowej. Ze względu na sposób działania oraz techniki tworzenia wirusy można podzielić na utajnione i polimorficzne.

Wirusy utajnione wykorzystują jedną z wielu technik ukrywania swojej obecności na dysku twardym. Gdy system operacyjny odwołuje się do pewnych informacji, wirus przekazuje wersję tejże informacji sprzed infekcji, tzn. wirus zapisuje informacje potrzebne do późniejszego oszukania systemu operacyjnego i programów antywirusowych. Wirusy polimorficzne z kolei mogą się zmieniać lub inaczej mutować, co czyni je trudniejszymi do zidentyfikowania. Działanie takie oznacza, że suma kontrolna, po której przeszukiwane są pliki w celu odnalezienia infekcji, jest zmienna. Mutacja wirusa polega więc na zmianie jego rozmiarów i struktury. Dobrze napisany wirus polimorficzny może być bardzo trudno wykrywalny, ponieważ większość programów antywirusowych poszukuje w badanych plikach odpowiednich ciągów i wartości zawartych w ich bazie wirusów, na które składają się m.in. rozmiar, suma kontrolna, data i inne [Dudek 1998].

Oprócz wirusów infekujących pliki wykonywalne istnieją tysiące innych rezydujących w plikach danych. Są to tzw. wirusy makr, infekujące między innymi pliki dokumentów generowanych przez edytor Microsoft Word i arkusz kalkulacyjny Excel. Takie wirusy zazwyczaj atakują globalne szablony dokumentu, ostatecznie uszkadzając każdy otwarty dokument edytora Word lub arkusza kalkulacyjnego Excel.

Według CERT NASK intruzi włamujący się do systemów w Polsce najczęściej przeprowadzali następujące działania:

- wprowadzanie zmian w zaatakowanym systemie, takich jak modyfikacja plików haseł, podmienianie oprogramowania systemowego,
- instalację modułów typu koń trojański lub tzw. sniffer – podsłuchiwanie pakietów TCP/IP,
- ingerencję w prywatność, objawiającą się najczęściej przeglądaniem cudzej poczty elektronicznej,
- powodowanie szkód moralnych i załamań systemów komunikacyjnych, takich jak zmiana zawartości stron WWW, rozsyłanie niechcianej korespondencji.

Działania umyślne stanowią tylko część całości zagrożeń systemów komputerowych, do których zaliczyć można również zachowania nieświadome, powodujące awarie systemu.

5. Kierunki zabezpieczeń systemów informatycznych

Biorąc pod uwagę bezpieczeństwo oferowanych usług, dobry system informatyczny powinien obejmować [Grzywacz 2003]:

- ochronę informacji przed utratą lub zniekształceniem przez tworzenie kopii zapasowych i stosowanie tzw. zapisów zwierciadlanych, tzn. zapisywanie tych samych danych jednocześnie na dwóch nośnikach,
- zabezpieczenie przed nadużyciem danych, czyli uniemożliwienie osobom nieupoważnionym dokonywania operacji na danych oraz dostępu do jakichkolwiek danych podlegających ochronie prawnej,
- przygotowanie systemu do działania na wypadek awarii, uszkodzenia programu lub sprzętu komputerowego.

Aby zabezpieczyć swój system informatyczny przed zagrożeniami ze strony koni trojańskich, robaków internetowych i wirusów, należy mieć zainstalowane w systemie aktualne oprogramowanie antywirusowe. Reaguje ono zwykle na wzory wirusów, dlatego trudne jest osiągnięcie całkowitego bezpieczeństwa systemu. Dobry program antywirusowy powinien zapewnić:

- aktywne skanowanie – dzięki tej funkcji moduły programu antywirusowego ciągle działają, w tle skanując otwierane pliki,
- monitorowanie poczty – funkcja ta pozwala na wyszukiwanie wirusów w załącznikach otrzymywanych wiadomości elektronicznych,
- bieżąca aktualizacja definicji wirusów – wykorzystywany jest tutaj proces automatycznej aktualizacji w celu uzyskania najświeższych sygnatur wirusów. Mechanizmy bieżącej aktualizacji mogą automatycznie wyszukiwać nowe aktualizacje na witrynie producenta, pobierać je oraz instalować nową bazę danych.

Techniki zabezpieczeń systemów informatycznych można podzielić na organizacyjne, administracyjne, fizyczne oraz programowe. Przygotowanie organizacyjne polega na prawidłowej organizacji procesów pracy oraz określeniu kompetencji pracowników. Określa się tutaj procedury awaryjne, informujące o zachowaniu się pracowników w przypadku awarii sprzętu, sieci komputerowej, włamania, pożaru [Nowicki 2002].

Techniki administracyjne polegają na certyfikowaniu oraz odpowiednim zarządzaniu dostępem do pomieszczeń. Poszczególni użytkownicy powinni mieć również nadane odpowiednie uprawnienia. Podmioty certyfikujące powinny posiadać kwalifikacje, doświadczenie i renomę. Każde przedsiębiorstwo musi mieć procedury regulujące godziny i dostępność kluczy do pomieszczeń. Powinna być także ustalona lista pracowników, którzy mogą je pobierać. Pomocne tutaj mogą być zamki z urządzeniami identyfikującymi użytkownika [Nowicki 2002]. Zabezpieczenia fizyczne to oprócz zabezpieczeń mechanicznych wszelkiego rodzaju zabezpieczenia transmisyjne i emisyjne. Wiąże się to z używaniem sprzętu posiadającego certyfikaty świadczące o obniżonej emisji fal elektromagnetycznych, stosowaniem dodatkowego ekranowania kabli i sprzętu w przypadkach tego wymagających, całościowym ekranowaniu pomieszczeń.

Do technik programowych zabezpieczających informacje przechowywane i przetwarzane w systemach informatycznych należą: identyfikacja, autoryzacja i kontrola dostępu. Identyfikacja polega na przydzieleniu każdemu użytkownikowi

systemu identyfikatora. Prawie każdy system informatyczny posiada również proces uwierzytelniania, opierający się na podaniu, oprócz identyfikatora użytkownika, odpowiedniego hasła. Ważna jest też autoryzacja, którą nazywamy proces przydzielania praw dostępu poszczególnym użytkownikom. Polega on na ustaleniu, czy dana osoba może mieć dostęp do plików i na jakim poziomie. Kontrola dostępu to usługa, z której korzystają administratorzy w celu ustalenia praw dostępu do sieci i zasobów. Określa, kto i pod jakim warunkiem może korzystać z określonego zasobu [Nowicki 2002].

Z kolei najlepszym sposobem na zabezpieczenie systemów informatycznych w lokalnej sieci komputerowej przed atakami z Internetu jest zastosowanie zapory sieciowej lub inaczej firewala. Jest to urządzenie zaprojektowane do zapobiegania niepowołanemu dostępowi do sieci, którym zazwyczaj jest niezależny komputer, router lub inny sprzętowy element sieci, jak również odpowiednie oprogramowanie. Zapora stanowi jedyny punkt wejścia do sieci lokalnej danego przedsiębiorstwa bądź instytucji. Jej zadaniem jest kwalifikacja nadchodzących z zewnątrz zgłoszeń według zadanych reguł i ich przetworzenie, co w najprostszym ujęciu sprowadza się do akceptacji bądź odrzucenia żądania połączenia z danym serwerem usług sieciowych [Atkins 1997]. Można wyróżnić dwa podstawowe typy zapór sieciowych: zapory sieciowe na poziomie sieci/pakietu, którymi są zazwyczaj routery z możliwościami filtrowania pakietów. Administrator korzystający z takiej zapory ma możliwość przyznania bądź odmowy dostępu do swego serwera na podstawie kilku zmiennych. Są to m.in.: adres źródłowy, protokół, zawartość, numer portu. Routery mają możliwość translacji/konwersji protokołów – tzw. NAT, czyli network address translation. Drugim typem zapór są zapory sieciowe na poziomie aplikacji/usługi tzw. bramy pośredniczące proxy.

6. Rezultaty badań z dziedziny bezpieczeństwa danych w systemach informatycznych

Na początku maja 2004 r. Georg Grohs, konsultant ds. informatyki z firmy Inceon na zlecenie Symantec Polska opracował raport dotyczący bezpieczeństwa danych w sieci Internet. Stworzono go na podstawie logów dostarczonych przez ponad 1000 polskich użytkowników programu Norton Internet Security oraz wypełnionych przez nich później kwestionariuszy. Z raportu wynika, iż blisko połowa (498 osób) uczestników badania przyznała, że przed jego rozpoczęciem stali się celem ataku przeprowadzonego za pośrednictwem Internetu – z tego u 109 osób efektem ataku było uszkodzenie systemu, 56 zaś straciło ważne dane. Z opracowania wynika też, iż zdecydowana większość badanych użytkowników korzysta stale z oprogramowania antywirusowego i firewall. Tylko co 9 użytkownik nie korzystał z żadnych programów zabezpieczających. Co ważne, ok. 30% (363) użytkowników uważa, że w czasie surfowania po sieci są wysoce narażeni na jakieś zagrożenie, a zdecydowana większość (673 użytkowników) uważa, że „jakieś" ryzyko istnieje [Cieślak 2004].

W najnowszym raporcie Symanteca obejmującego okres od 1 stycznia do 30 czerwca 2005 r. wskazano na wzrost liczby ataków DoS (Denial-of-Service) w stosunku do roku poprzedniego. Firma Symantec wykryła 1862 nowe luki bezpieczeństwa, co jest najwyższą liczbą w historii badań tejże firmy. Wzrosła także liczba odmian wirusów i robaków atakujących platformę Win32, wykryto 10 866 nowych odmian wirusów i robaków. Każdego dnia obserwowano średnio 10 352 aktywne komputery zainfekowane oprogramowaniem typu bot. Wykazano również, że 61% całego ruchu pocztowego stanowił spam oraz że 51% tego typu wiadomości pochodziło ze Stanów Zjednoczonych [Muszyński 2005]. Zanotowano również wzrastającą tendencję liczby zagrożeń skierowanych przeciwko sieciom bezprzewodowym.

Inny raport firmy iDefense, opublikowany w listopadzie 2005 r., analizuje problem keyloggerów, czyli aplikacji przechwytujących znaki wprowadzane za pomocą klawiatury i przekazujących je dalej, np. za pośrednictwem sieci Internet. Keyloger może przechwycić wprowadzane przez użytkownika numery karty kredytowej, hasła dostępu do banków internetowych, poczty elektronicznej itd. Raport mówi, iż w 2005 r. pojawiło się ponad 6 tys. takich programów, tj. 65% więcej aniżeli w roku 2004 [Cieslak 2005]. W raporcie tym znajdziemy informację, iż po zainstalowaniu w systemie keylogger przechwytuje dane niezbędne do zalogowania się do e-banku lub serwisu finansowego średnio w 81 godzin. W przypadku udanego włamania z wykorzystaniem keyloggera przeciętne straty poniesione przez użytkownika wynoszą 4 tys. dol.

Z raportu CERT Polska dostępnego w sieci Internet pod adresem www.cert.pl/ /raporty i dotyczącego roku 2004 wynika, że ponad połowa wszystkich obsłużonych przez tę organizację incydentów to przypadki dotyczące gromadzenia informacji (54,7%), a zwłaszcza skanowania. Dalsze przypadki to złośliwe oprogramowanie (13,5%) oraz nielegalne i obraźliwe treści (11,5%). Najmniej przypadków zostało odnotowanych w kategorii włamania 2,4% i oszustwa komputerowe 8,4%. W sumie CERT zewidencjonowała 1222 przypadki incydentów. Zanotowano także wzrost zjawiska nazywanego phisingiem, polegającego na zwabieniu użytkownika na spreparowaną stronę internetową, która wygląda tak samo jak strona banku albo strona innego serwisu wymagającego uwierzytelnienia, a następnie nakłonieniu go do zalogowania się na takiej stronie. W taki sposób od nieświadomego użytkownika podstępnie wydobywane jest hasło i login. Jeśli weźmiemy pod uwagę ogólną liczbę incydentów w latach 2000-2004, to zauważymy tendencję rosnącą, a mianowicie w roku 2000 zanotowano 126 przypadków incydentów naruszenia bezpieczeństwa, w roku 2001 – 741 przypadków, 2002 r. – 1013 incydentów, w 2003 r. – 1196, a w 2004 r. – jak już wspomniano 1222 przypadki. Przede wszystkim wzrosła aktywność wirusów, szczególnie takich jak MyDoom, Beagle, Netsky oraz robaków internetowych, takich jak Sasser, Witty i Dabber.

7. Zakończenie

Współczesne technologie informacyjne rozwijają się bardzo szybko, wprowadzane są ciągle nowe zabezpieczenia. Konieczne staje się kompleksowe myślenie o bezpieczeństwie i kompleksowe jego wdrażanie. Należy również pamiętać, iż najsłabszym ogniwem systemu informatycznego jest człowiek, którego zawodność pracy jest często o wiele większa niż zawodność systemów informatycznych. Zagrożenia, na jakie narażony jest system informatyczny, można podzielić na następujące klasy: uzyskanie dostępu przez osoby niepowołane do danych przesyłanych przez sieć lub przechowywanych w komputerach, utrata danych na skutek działań z zewnątrz, fałszerstwo danych, uniemożliwienie korzystania z pewnych usług i zasobów przez legalnych użytkowników. Jak wynika z przedstawionych raportów, z roku na rok zwiększa się zagrożenie, na jakie wystawiane są systemy informatyczne. W głównej mierze dotyczy to systemów podłączonych do sieci rozproszonych jak Internet. W celu zabezpieczenia systemu informatycznego przed zagrożeniami należy dbać o instalację aktualnych łat systemowych, uaktualniać oprogramowanie antywirusowe oraz odpowiednio przeszkolić pracowników i zapewnić właściwą politykę bezpieczeństwa danych w organizacji.

Literatura

Atkins D., *Bezpieczeństwo Internetu – profesjonalny informator*, Oficyna Wydawnicza LT&T, Warszawa 1997.

Cieślak D., *Polski Internet: raport o stanie zagrożenia*, http://www.pcworld.pl/news/ news. asp?id=66447, maj 2004.

Cieślak D., *Uwaga, szpiedzy obserwują klawiatury!*, http://www.pcworld.pl/news/85371.html, listopad 2005.

Dudek A., *Nie tylko wirusy*, Wydawnictwo Helion, Gliwice 1998.

Grzywacz J., *Bezpieczeństwo systemów informatycznych w bankach w Polsce*, Oficyna Wydawnicza SGH, Warszawa 2003.

Molski M., Opala S, *Elementarz bezpieczeństwa systemów in*formatycznych, Mikom, Warszawa 2002.

Muszyński J., *Symantec: raport na temat zagrożeń w Internecie*, http://www.pcworld.pl/news/85233.html, listopad 2005.

Niezgódka J., *Jak bronić się przed hackerami*, Komputerowa Oficyna Wydawnicza HELP, Warszawa 1999.

Nowicki A. (red.), *Wstęp do systemów informacyjnych zarządzania w przedsiębiorstwie*, Wydawnictwo Politechniki Częstochowskiej, Częstochowa 2002.

Nowicki A., Unold J. (red.), *Organizacyjne aspekty doskonalenia systemów informacyjno-decyzyjnych zarządzania*, AE, Wrocław 2002.

Nowicki A., Ziora L., Rot A., *Information Security Policy: The Polish Financial Institutions Case*, ITIB International Conference, St. Petersburg, June 2005.

Scambray J., McClure S., Kurtz G., *Hakerzy cała prawda*, Translator, Warszawa 2001.

THE CHOSEN ASPECTS OF DATA SECURITY IN INFORMATION SYSTEMS

Summary

The aim of this article is to present classification of threats of Information Systems and directions of their protections. The article defines the notion of data security and explains such terms within the scope of data security as modification, destruction, copying, confidentiality, inviolability of data. The paper presents also international standards of security classes. The research results included in the article come from reports elaborated by CERT Poland, iDefense and Symantec enterprise.

Leszek Ziora – mgr, doktorant studiów zaocznych przy Wydziale ZI Akademii Ekonomicznej we Wrocławiu.