PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1081 — 2005
Nowoczesne technologie informacyjne w zarządzaniu

Kamal Matouk

WIELOPOZIOMOWY MODEL BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO ZARZĄDZANIA

1. Wprowadzenie

Zapewnienie bezpieczeństwa systemów informatycznych i znajdujących się w nich informacji jest niezbędne w każdej instytucji. Wymagania prawa nakładają na firmy i wszystkie inne organizacje obowiązek podjęcia szeregu działań o charakterze organizacyjnym i technicznym w zakresie ochrony systemów i przetwarzanych w nich informacji. Prawdą jest, że rozwój technologii informatycznych i upowszechnienie Internetu z jednej strony sprawiły, że:

- dostęp do wszelkich rodzajów informacji stał się nie tylko możliwy, ale i łatwy do uzyskania dla wszystkich firm,
- badanie rynku i zbieranie informacji o klientach jest dużo łatwiejsze i szybsze niż kiedykolwiek wcześniej,
- publikacja informacji o firmie (raporty, promocje, oferty pracy i inne) jest szybka i tania dla wszystkich;

z drugiej jednak spowodowały, że:

- zagrożenie włamaniem do systemów z zewnątrz i utratą danych jest duże,
- wymagania dotyczące ochrony systemów są znacznie większe i staranniej kontrolowane przez firmy.

Wraz z rozwojem technologii i komplikacją systemów informatycznych liczba potencjalnych zagrożeń bezpieczeństwa systemów organizacji i ich danych stale rośnie. Coraz więcej osób posiada dostęp do Internetu, co sprawia, że prawdopodobieństwo włamania do najbardziej chronionych zasobów organizacji, uszkodzenia systemów i zniszczenia danych jest większe. W związku z tym wszyscy pracownicy firmy, zarówno administratorzy systemu informatycznego, jak i użytkownicy, powinni być świadomi, że ochrona systemu informatycznego i danych w nim zgromadzonych, jest sprawą pierwszorzędną, którą należy traktować poważnie. Badania przeprowadzone w stolicy jednego z europejskich krajów w

2004 r. wykazały, że blisko trzy czwarte pracowników biurowych zdradziłoby swoje hasło do sieci korporacyjnej w zamian za czekoladowego batonika [Interia, Internet 2004a]. Wyniki tego eksperymentu świadczą, że pracodawcy przykładają zdecydowanie zbyt małą wagę do szkoleń swoich pracowników w zakresie bezpieczeństwa, wdrażania oraz uaktualniania odpowiednich procedur ochrony w miejscach pracy.

Dobry plan ochrony nie może zagwarantować bezpieczeństwa systemu informatycznego (sprzętu i informacji) bez wsparcia technicznego oraz odpowiedniego szkolenia pracowników. Dodatkowo plan ten musi uwzględniać, że zakres odpowiedzialności za system informatyczny organizacji powinien zostać podzielony tak, aby nikt nie miał nad nim wyłącznej kontroli.

W dalszej części artykułu podkreślono konieczność planowania ochrony systemu informatycznego zarządzania oraz przedstawiono strategię ochrony.

2. Przesłanki bezpieczeństwa systemu informatycznego

Bezpieczeństwo systemu informatycznego (BSI) jest pojęciem szerokim (więcej na ten temat w [Barczak, Sydoruk 2003]), które wymaga określenia pewnych warunków, do których należą (por. [AltKom, Internet 2005a]):

- kluczowe zasoby organizacji i ich wartości,
- poziom dopuszczalnego ryzyka utraty i uszkodzenia danych,
- platforma techniczna systemu ochrony.

Do dnia dzisiejszego wiele firm nie tylko w Polsce, ale i na świecie, funkcjonując na rynku, nie ma jeszcze wdrożonej polityki bezpieczeństwa oraz wbudowanego systemu zarządzania bezpieczeństwem (szerzej w [Sadowski 2000]). Firmy te, zamiast finansować przedsięwzięcia, które wydają im się abstrakcyjne, wolą wydawać pieniądze na to, co jest namacalne i w zauważalny sposób podnosi komfort pracy.

Należy jednak pamiętać, że każda poważna awaria powodująca brak dostępu do systemu informatycznego firmy, penetracja zewnętrzna lub utrata poufnych danych mogą spowodować ogromne koszty bezpośrednie, a także straty niematerialne w postaci np. utraty zaufania do firmy, co w konsekwencji przyczynia się do utraty klientów. Dlatego od pewnego czasu zabezpieczenie systemów informatycznych stało się obowiązkiem działu informatycznego każdej organizacji. Zadaniem tego działu jest planowanie sposobów zapobiegania oraz szybkiej reakcji na zagrożenia w chwili pojawienia.

Firmy obecnie stosują różne sposoby zabezpieczenia swoich systemów, np. ścianę ogniową (*firewall*) czy procedury *backupu*. Jednak takie zabezpieczenia nie są wystarczające. Pojedyncze elementy ochrony środowiska informatycznego, które mają chronić dane podczas ataku, mogą nie sprostać zapewnieniu dostępności np. w razie awarii. Dlatego niezbędna jest właściwa architektura rozwiązań technicznych oraz dobrze przygotowany plan ochrony.

3. Filary bezpieczeństwa danych w systemie

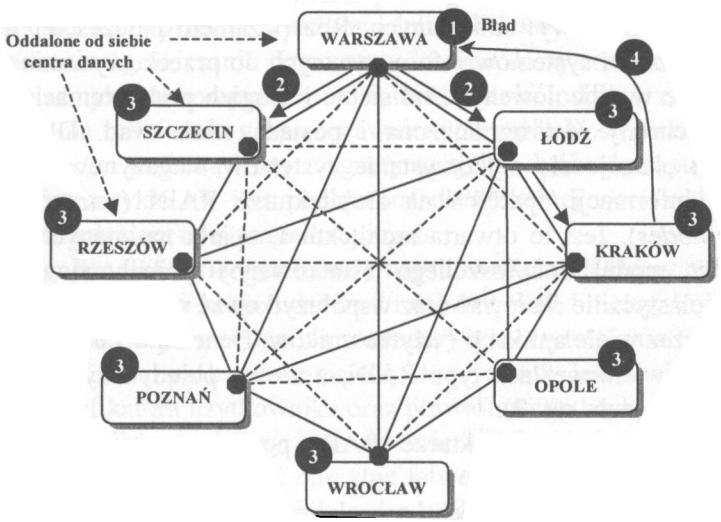
Informacje przechowywane w systemie informatycznym są jednymi z najbardziej wartościowych zasobów organizacji, które należy chronić. Myśląc o ochronie systemu informatycznego, zazwyczaj bierze się pod uwagę ochronę zasobów informacyjnych systemu przed osobami zewnętrznymi, czyli spoza firmy, np. przed konkurencją. Często jednak największą korzyścią płynącą z dobrze zaprojektowanego systemu ochrony jest zabezpieczenie przed ciekawością uprawnionych użytkowników wewnętrznych, jak również ochrona przed uszkodzeniami danych w systemie – można bowiem niechcący usunąć z systemu ważny plik lub zbiór danych, który nie jest dostatecznie chroniony. Wprowadzenie strategii ochrony w organizacji ma zapewnić bezpieczeństwo informacji, polegające na jej zabezpieczeniu przed przypadkowym lub umyślnym zniszczeniem, ujawnieniem lub modyfikacją. Główne powody ochrony zasobów informacyjnych organizacji, zwane inaczej filarami bezpieczeństwa, są następujące (por. [*Podstawy ochrony...* Internet 2004d; Werner 2003]):

- **Poufność danych** – właściwe środki ochrony mogą zapobiec przeglądaniu poufnych informacji przez osoby niepowołane lub ujawnianiu ich.
- **Integralność danych** – zapobieganie nieuprawnionym zmianom czy usuwaniu danych gwarantuje do pewnego stopnia integralność danych w systemie informatycznym.
- **Dostępność danych** – niedopuszczanie do uszkodzenia danych w systemie umożliwia stały do nich dostęp. W sytuacji przypadkowego lub umyślnego uszkodzenia danych nie można uzyskać do nich dostępu aż do czasu ich ponownego odtworzenia.

Bezpieczeństwo systemów informatycznych wymaga także spełnienia następujących trzech warunków (por. [IT-SCS, Internet 2005b]):

- **Autentyczność** – jest to proces gwarantujący, że osoba uzyskująca dostęp do systemu jest faktycznie tą, której przyznano prawo dostępu. Do tego celu służą hasła, metody biometryczne i certyfikaty cyfrowe.
- **Rozliczalność** – oznacza powiązanie zdarzeń w systemie z konkretnym użytkownikiem, który te zdarzenia spowodował. Jest to warunek konieczny dla systemów informatycznych przechowujących informacje tajne lub poufne (np. transakcje finansowe, rachunki bankowe, dane osobiste).
- **Niezaprzeczalność** – jest bardzo istotna z uwagi na możliwość monitorowania poczynań wszystkich użytkowników, a nawet administratora systemu, i jest ściśle powiązana z poprzednimi warunkami. System zapamiętuje szczegółowo wszystkie akcje, czynności i transakcje wykonane przez użytkowników w zaszyfrowanych plikach, a osoba, która dokonała czynności, nie będzie w stanie zaprzeczyć, iż akcja miała miejsce i została wykonana przez tę właśnie osobę.

Rys. 1. Filary bezpieczeństwa systemów informatycznych zarządzania
Źródło: opracowanie własne.



1 – Węzeł w Warszawie stwierdza uszkodzenia jednego z jego plików.
2 – Węzeł wysyla żądanie replikowania uszkodzonego plików do wszystkich pozostałych węzłów.
3 – Wszystkie węzły odbierają żądanie i sprawdzają, czy dysponują tym plikiem oraz czy nie jest on uszkodzony
4 – Replika pliku zostaje odnaleziona w zasobach Krakowa; węzeł w Warszawie odczytuje go i zapisuje w swoich zasobach

Rys. 2. Zasady działania architektury RAIN
Źródło: opracowanie własne na podstawie [NetWorld, Internet 2004c].

Warto zauważyć, że ominięcie jednego z wyżej wymienionych filarów bezpieczeństwa zazwyczaj powoduje upadek pozostałych. Dlatego strategia ochrony systemu musi dotyczyć wszystkich aspektów (warunków) bezpieczeństwa i wprowadzić w nich odpowiednie wzmocnienie. Filary bezpieczeństwa systemów przedstawiono na rys. 2.

4. Wielopoziomowy model ochrony systemu informatycznego

Jedna z podstawowych strategii bezpieczeństwa polega na zapewnianiu ochrony systemu informatycznego przez stosowanie wielopoziomowego modelu ochrony. Polega to na podzieleniu ochrony na określone części, które można planować, zarządzać nimi i monitorować. Z punktu widzenia administratora, a także użytkownika systemu informatycznego, ochronę można podzielić na następujące poziomy:

- platformy technologicznej,
- ochrony fizycznego dostępu do systemu,
- legalizacji i uwierzytelnienia użytkowników,
- uprawnień użytkowników,
- szkolenia i uświadomienia użytkowników.

Poziom platformy technologicznej. Jest to poziom, który określa platformy technologiczne przechowywania danych. Rozwiązaniem najczęściej wykorzystywanym w większości systemów informatycznych do przechowywania danych jest ich zapisywanie w odizolowanych od siebie i drogich podsystemach dyskowych. Ta metoda ochrony jest ograniczona i posiada wiele wad. Dlatego dobrym rozwiązaniem okazuje się wykorzystanie systemów magazynowania, ochrony i uzyskiwania informacji opartych na architekturze RAIN (*redundant array of inexpensive nodes*). Jest to otwarta architektura, oparta na znanych standardach, służąca jako model rozproszonego (siatkowego) przechowywania danych, pozwalająca elastycznie skalować oraz współużytkować wszystkie przechowywane w niej dane przez wiele aplikacji i użytkowników. Dane są w takim systemie przechowywane na wielu węzłach typu RAIN, a nie na pojedynczych podsystemach pamięci masowej (zob. rys. 2).

Typowy system o architekturze RAIN posiada następujące cechy (por. [NetWorld, Internet 2004c]):

1. Węzły systemu to najczęściej kompaktowe serwery z pojemnymi dyskami twardymi, szybkimi portami sieciowymi i wydajnym procesorem.
2. Warstwa połączeń międzysieciowych oparta na protokole IP, co pozwala administratorowi zbudować sieć zintegrowanych ze sobą węzłów. Węzły te mogą być zlokalizowane w wielu oddalonych od siebie centrach danych.
3. Oprogramowanie wykorzystywane w systemie RAIN do stałej komunikacji i wymiany informacji między węzłami potrafi samo automatycznie wykrywać obecność nowego węzła RAIN i go skonfigurować. Potrafi także tworzyć wirtualną pulę zasobów i zarządzać nią bez udziału administratora.
4. Oprogramowanie zarządzające cyklem „życia" informacji w systemie oferuje zaawansowane rozwiązania do kompresowania i szyfrowania danych, oznaczania wersji danych, sprawdzania spójności danych i usuwania błędów w przypadku ich wykrycia. Natomiast mechanizmy replikowania danych oparte na specjalnych algorytmach pozwalają replikować dane na wiele węzłów.

5. Siatka węzłów systemu może się adaptować do zmieniających się warunków pracy poszczególnych aplikacji, które mogą korzystać raz intensywnie, innym razem mniej intensywnie z usług pamięci masowych, rozkładając w różny sposób obciążenie zadaniami poszczególnych węzłów.
6. Każdy węzeł w systemie sprawdza regularnie stan wszystkich swoich plików danych. W przypadku natrafienia na uszkodzony plik węzeł inicjuje żądanie replikowania danych i wysyła je do wszystkich pozostałych węzłów, które weryfikują własne repliki i współpracują ze sobą kolektywnie w celu odzyskania uszkodzonego pliku.

Systemy ochrony korzystające z powyższej architektury mogą zapewnić użytkownikom stały i niezawodny dostęp do danych.

Poziom ochrony fizycznego dostępu. Ochrona fizyczna systemu jest w większości przypadków zapewniona poza systemem i zabezpiecza jednostkę systemową, wszystkie urządzenia systemowe oraz nośniki składowania (dyskietki, taśmy, dyski CD i inne) przed przypadkową lub celowo wywołaną utratą danych.

Wprowadzenie ograniczania fizycznego dostępu do systemu może być zrealizowane przez zamykanie komputerów w pomieszczeniach dobrze chronionych, do których dostęp ma tylko mała grupa uprawnionych osób. Dostęp odbywa się przy uwierzytelnieniu (za pomocą karty magnetycznej, lub kodu dostępu). Większość takich systemów zwykle nie jest podłączona do globalnej sieci komputerowej i korzysta z własnych sieci telekomunikacyjnych.

Poziom legalizacji i uwierzytelnienia użytkowników. Kolejny poziom modelu ma na celu zapewnienie bezpieczeństwa i ochronę przed nielegalnym dostępem użytkowników do systemu za pomocą procedury uwierzytelniania (najczęściej za pomocą haseł). Każda próba dostania się do systemu jest związana z wprowadzeniem identyfikatora użytkownika oraz prawidłowego hasła dostępu. Wszystkie hasła użytkowników powinny być odpowiednio kontrolowane na etapie ich tworzenia, ponieważ nie może być ono zbyt łatwe do odgadnięcia. Krótkie hasła i te, które wywodzą się z nazwy lub opisu użytkownika, nie są dopuszczalne [Sadowski, Internet 2004e].

Istnieją jeszcze inne metody uwierzytelniania, takie jak korzystanie z inteligentnych kart lub specjalnych modemów. Temat ten szerzej opisany w [Kowalkiewicz, Internet 2002].

Poziom uprawnień użytkowników. Poziom uprawnień wymaga, aby każdy użytkownik systemu miał swój profil, za pomocą którego można danemu użytkownikowi zawęzić dostęp do określonego zbioru, programu, menu lub kilku funkcji systemowych.

- Na poziomie zbiorów i programów można sprecyzować, czy użytkownik ma uprawnienia tylko do przeglądania informacji w zbiorze, czy do zmiany danych bądź do zmiany i usunięcia całego zbioru czy pojedynczego programu.
- Na poziomie funkcji systemu umożliwiającej zapisywanie i odtwarzanie informacji, zarządzanie wydrukami oraz konfigurowanie nowych użytkow-

ników systemu zabezpieczenie może określić, które z najczęściej używanych funkcji systemowych dany użytkownik może wykonywać.

Dodatkowo wydajność systemu informatycznego firmy jest sprawą bardzo ważną, dlatego należy dopilnować, aby użytkownicy nie nadużywali zasobów systemu, zajmując np. zbyt dużo pamięci na dyskach.

Poziom szkolenia i uświadomienia użytkowników. Podstawą ochrony systemu informatycznego przedsiębiorstwa jest szkolenie, pogłębianie wiedzy i świadomości pracowników w zakresie ochrony.

Zazwyczaj najsłabszym elementem systemu bezpieczeństwa w firmie jest człowiek. Wszystkie błędy popełnione przez pracownika mogą wynikać z braku odpowiedniej świadomości istniejących zagrożeń. Techniki wykorzystujące ludzkie słabości znane są pod nazwą *social engineering* [Uniewski, Internet 2004f]. Istnieją dwa sposoby oszukania użytkownika. Pierwszy to użycie środków programowo-sprzętowych, np. rozmieszczenie stron zawierających odpowiednio umotywowaną prośbę o podanie identyfikatora użytkownika oraz hasła. Natomiast drugi bazuje na bezpośrednim kontakcie telefonicznym lub osobistym z użytkownikiem.

5. Zakończenie

W dobie rozwoju Internetu oraz ewolucji technologii przetwarzania danych zapewnienie optymalnego bezpieczeństwa systemów informatycznych (sprzętu, oprogramowania i informacji) staje się zadaniem coraz trudniejszym i bardziej złożonym. Utrata danych czy zniszczenie ważnych informacji może zagrażać funkcjonowaniu, a nawet istnieniu przedsiębiorstwa. Dawniej możliwości transferu danych były ograniczone. Obecnie prędkość przenoszenia informacji zwiększyła się do stopnia praktycznie uniemożliwiającego kontrolę. Ponadto większość powszechnie stosowanych systemów operacyjnych (z wyjątkiem komputerów typu *mainframe*) nie posiada mechanizmów pozwalających na ograniczenie działań użytkownika (np. kopiowania plików na nośniku). W związku z tym podstawą ochrony systemów komputerowych przedsiębiorstwa staje się wprowadzenie odpowiedniej strategii bezpieczeństwa. Zaprojektowanie i wdrożenie strategii ochrony zależy od konkretnego przedsiębiorstwa i jego specyfiki.

Literatura

AltKom, *Bezpieczeństwo systemów informatycznych*, materiały firmowe, http://www.altkom.com.pl/bezpieczenstwoIT/, 14-02-2005, Internet 2005a.

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

Interia.pl, *Piractwo w sieci, batonik – tajną bronią*, http://www.interia.pl z 22-04-2004, Internet 2004a.
IT-SCS, *Bezpieczeństwo systemu informatycznego*, materiały firmowe, http://www.it-scs.com.pl/zabezpiecz1.html, z 19-04-2005, Internet 2005b.
Kerberos, *Przedmioty ochrony w systemie informatycznym*, http://www.bezpieczenstwoit.pl/Artykuly/Polityka_Bezpieczenstwa/, z 4-06-2004, Internet 2004b.
Kowalkiewicz M., *Zabezpieczenia usług bankowych poprzez Internet po stronie klienta – rozwiązania stosowane w Polsce*, http://www.gazeta-it.pl/archiwum/git08/ zabezpie-czenia.html", Gazeta IT, grudzień 2002, nr 8, Internet 2002.
NetWord, *Architektura RAIN*, http://www.networld.pl/artykuly/40461.html, Net Word, z 01-04-2004, Internet 2004c.
Podstawy ochrony systemu, http://publib.boulder.ibm.com/html/as400/v5r1/ic2978 /index.htm?info/rbapk/rbapkrbapk001understandingsec.htm, z 12-05-2004, Internet 2004d.
Sadowski A., *Czym jest polityka bezpieczeństwa organizacji?* [w:] *II Seminarium polityki bezpieczeństwa*, Kerberos, Warszawa 2000.
Sadowski A., *Strategie realizacji polityki bezpieczeństwa*, http://www. Bezpieczenstwoit.pl/Artykuly/Polityka_Bezpieczenstwa/, Kerberos, z 21-05-2004, Internet 2004e.
Uniewski J., *Social Engineering – sposób na zdobycie informacji*, http://www.bezpieczenstwoit.pl/Artykuly/Bezpieczenstwo_sieci/, z 4-06-2004, Internet 2004f.
Werner J., *Bezpieczeństwo systemów informatycznych*, PTI Forum, Toruń 2003.

LAYER SECURITY MODEL OF THE MANAGEMENT INFORMATION SYSTEM

Summary

The article presents issues relating to Management Information Systems protection strategy in enterprises and highlights the important of planning system security and its content. Therefore, I propose a layer protection system which I believe that will help enterprises in planning their security system.

Dr inż. Kamal Matouk jest adiunktem w Katedrze Informatyki Ekonomicznej Akademii Ekonomicznej we Wrocławiu
e-mail: kamal.matuk@ae.wroc.pl