ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1998
Seria: INFORMATYKA z. 34 Nr kol. 1381

Katarzyna TRYBICKA, Adam ZIĘBIŃSKI
Politechnika Śląska, Instytut Informatyki

ZAGADNIENIA BEZPIECZEŃSTWA W SYSTEMIE OBIEGU INFORMACJI MULTIMEDIALNEJ URZĘDU MIASTA PSZÓW

Streszczenie. Opracowanie poświęcone jest problemom bezpieczeństwa i ochrony zasobów w rozbudowanym, multimedialnym systemie obiegu informacji. Zaakcentowano problemy związane z tworzeniem i integracją lokalnych sieci komputerowych oraz dołączeniem ich do sieci Internet; przedstawiono metody zabezpieczania zasobów przed atakami zewnętrznymi, jak i wewnętrznymi. Zaprezentowane rozwiązania są wdrażane w Urzędzie Miasta Pszów.

PROBLEMS OF SECURITY IN A MULTIMEDIA INFORMATION EXCHANGE SYSTEM IN MUNICIPAL OFFICE OF THE CITY OF PSZÓW

Summary. Paper is devoted to problems of security of resources in a large multimedia information exchange system, with special accent given to the problems of building and integration of local area networks and connecting them to Internet. Methods for security of resources against external as well as internal attacks are presented. The solutions proposed in the paper are being implemented in municipal office of the city of Pszów.

1. Wstęp

Postęp technologii komputerowej wymusza projektowanie systemów komputerowych, które pozwalają na dalszy rozwój zastosowanych rozwiązań. Musi wiec być zgodny ze światowymi standardami, trendami rozwojowymi i przede wszystkim niezawodny w działaniu.

Założeniem przyjętym przez projektantów było, że system komputerowy Urzędu Miasta Pszów powinien:

- być podstawowym narzędziem codziennego użytku, służącym do komunikowania się między pracownikami,
- udostępniać zasoby informacyjne sieci Internet tym pracownikom urzędu, którzy akurat takiej usługi potrzebują,
- świadczyć szeroko rozumiane usługi informacyjne dla interesantów i mieszkańców miasta,
- służyć jako środek promocji miasta.

Do realizacji powyższych założeń celowe wydaje się zastosowanie w lokalnej sieci komputerowej (intranet) technologii i narzędzi powstałych dla sieci Internet, służące do wymiany poczty elektronicznej, tworzenia elektronicznych tablic ogłoszeniowych, aplikacji opartych na technologii WWW i bazach danych [4].

2. Strategia bezpieczeństwa

Nie można stworzyć całkowicie otwartej sieci realizującej jednocześnie postulat bezpieczeństwa, tak samo jak stworzenie sieci całkowicie bezpiecznej wyklucza, jak na razie, jej otwartość. Zmuszeni do przyjęcia wynikających z tego kompromisów projektanci sieci realizują postulat bezpieczeństwa w oparciu o kanon, który mówi, że na bezpieczeństwo sieci składają się :

- **Identyfikacja użytkownika**. Należy sprawdzić, czy nawiązano kontakt z właściwym węzłem oraz zidentyfikować użytkownika. Identyfikacja odbywa się programowo, na przykład za pomocą hasła lub sprzętowo urządzeniami takimi, jak karta magnetyczna, karta z procesorem itp. Sprawdza się również rodzaj upoważnienia do korzystania z zasobów.
- **Ochrona zasobów**, w tym ochrona danych realizowana na poziomie systemu oraz na poziomie sprzętu. Jest to problem rozpatrywany równolegle z identyfikacją użytkownika. Określa się sposoby i strategie zezwoleń na korzystanie z zasobów realizowane na przykład w formie haseł umożliwiających dostęp do nich.
- **Identyfikacja trasy**, zwana też **identyfikacją węzłów**. Zagadnienie to nabiera coraz większego znaczenia razem ze wzrostem rozproszenia terytorialnego sieci. Określa się prawdziwość węzłów biorących udział w sesji, ich wzajemne powiązania (zwane także poziomem zaufania), oraz wyznacza się grupy węzłów o takiej samej strategii bezpieczeństwa.
- **Ochrona sprzętu**. Ma na celu zapewnienie sprawności działania sieci, a co za tym idzie ochronę danych. Ochrona sprzętu realizowana jest na wielu poziomach: od wyboru okablowania po systemy dublowania serwerów. W kręgu zagadnień związanych

z ochroną sprzętu znajdują się systemy dyskowe (striping, duplexing, macierze RAID), zabezpieczenia przed awariami, fizyczna budowa sprzętu, dobór odpowiedniego serwera itd.

3. Lokalna sieć komputerowa

W kontekście elementów decydujących o bezpieczeństwie sieci, wymienionych w poprzednim punkcie, a także w ramach założeń, jakie ma spełniać projektowany system komputerowy dla Urzędu Miasta Pszów, twórcy zaproponowali sieć typu Microsoft Network, opartą na komputerach pracujących pod kontrolą systemów Windows NT i Windows 95 [2].

3.1. Windows NT

WindowsNT to 32-bitowy system operacyjny cechujący się wielozadaniowością, ochroną pamięci, realizujący wieloprocesowość symetryczną i posiadający mechanizmy sieciowe [3].

System WindowsNT ma szereg mechanizmów zabezpieczających dane przechowywane w jego systemie plików — przed nieupoważnionym dostępem i uszkodzeniem. Wszyscy użytkownicy muszą zarejestrować się w systemie podając nazwę swojego konta oraz hasło. Chroni to system plików przed dostępem osób niepowołanych. Administrator systemu może nałożyć na konto użytkownika szereg ograniczeń, na przykład ograniczyć możność zarejestrowania się do wyznaczonego fragmentu czasu lub też nakazać użytkownikowi zmianę hasła.

System WindowsNT ma również mechanizmy ochrony systemu plików, które wykrywają i eliminują uszkodzone sektory dysków oraz realizują ponownie transakcje, które zapisane zostały niekompletnie — na przykład z powodu przerwy w zasilaniu systemu. Tworzone są duplikaty informacji mających istotne znaczenie dla systemu plików — w celu zabezpieczenia się przed skutkami uszkodzenia sektorów, w których są przechowywane. Program instalacyjny tworzy również tzw. Dysk naprawczy, który może posłużyć do uruchomienia systemu w przypadku uszkodzenia informacji w rekordzie wprowadzającym (boot).

System WindowsNT spełnia wymagania bezpieczeństwa *Departament of Defense C2 Controlled Access Protection* [5], określone przez Departament Obrony USA. Klasa C2 narzuca konieczność implementacji w komputerach strategii bezpieczeństwa i śledzenia zdarzeń, obejmujących nie tylko kwestie dostępu, ze strony użytkowników sieci, ale również użytkowników lokalnych. Poziom bezpieczeństwa klasy C2 w systemie WindowsNT cechuje się następującymi możliwościami:

- Użytkownicy mają specjalne konta, wymagające rejestrowania się z podaniem hasła. Konto zawiera zapisy różnych czynności podejmowanych przez użytkownika, takich jak na przykład: zarejestrowanie się, wyrejestrowanie się i odwołanie się do plików.

Śledzone są również czynności dotyczące zarządzania, na przykład zmiany kont użytkowników lub parametrów pracy serwerów.

- Administratorzy i użytkownicy mogą sterować dostępem do plików, katalogów i zasobów (na przykład drukarek) swoich własnych systemów.
- Administratorzy systemów mogą śledzić kontrolowane wydarzenia.
- Użytkownicy nie mogą analizować zawartości pamięci operacyjnej.

Ponieważ WindowsNT pozwala na współdzielenie plików i zasobów, kwestie zabezpieczeń są istotne, jeśli do komputera ma dostęp wielu użytkowników. Administratorzy i użytkownicy muszą mieć możliwość zabezpieczenia współdzielonych plików przed nieuprawnionym wykorzystaniem. Zapewnienie bezpieczeństwa wiąże się z koniecznością wykonywania pewnych czynności natury administracyjnej. Muszą być nadane odpowiednie uprawnienia dotyczące współdzielonych katalogów, a administratorzy muszą utworzyć konta wymagające podania hasła, na które — w razie potrzeby — nałożone są dodatkowe ograniczenia możliwości rejestrowania się użytkownika.

Informacje dotyczące kont przechowywane są w głównej bazie danych, noszącej nazwę *Security Account Manager — SAM* — w każdym systemie WindowsNT. Gdy użytkownik rejestruje się w systemie, nazwa użytkownika i hasło sprawdzane są w bazie SAM systemu, w którym się użytkownik rejestruje.

O ile SAM zapewnia mechanizmy bezpieczeństwa, wystarczające w przypadku lokalnego systemu WindowsNT, pewne problemy pojawiają się przy zabezpieczeniu współdzielonych plików i zasobów znajdujących się na innych komputerach sieci. Możliwe jest na przykład określenie praw dostępu dla grupy użytkowników sieci, ale nie dla indywidualnych użytkowników, pracujących na innych komputerach. Jeśli zachodzi taka potrzeba, korzysta się z systemu WindowsNT Advanced Server [5].

WindowsNT Advanced Server ustala tzw. zasadę wzajemnego zaufania (ang. *trust relationships*) pomiędzy komputerami sieci. Oznacza to, że jeden komputer może zweryfikować użytkownika i przesłać informacje dotyczące użytkownika innym komputerom bez konieczności oddzielnego rejestrowania się w każdym.

Interesującą cechą systemu bezpieczeństwa jest fakt równoczesnego przekazu informacji dotyczącej plików razem z plikami. Na przykład — jeśli użytkownikowi zostanie nadane prawo otwarcia i odczytu pliku, bez prawa jego modyfikacji, te same prawa pozostaną w mocy nawet wtedy, gdy urządzenie przechowujące plik zostanie przeniesione do innego systemu.

WindowsNT Advanced Server udostępnia wiele możliwości, których brak w WindowsNT, na przykład większy stopień kontroli nad administrowanymi domenami i bardziej zaawansowane mechanizmy odporności na awarie. Te ostatnie obejmują między innymi

wsparcie dla systemu macierzy dyskowych RAID poziom 5 (zarówno zapis, jak i informacja kontrolna jest rozłożona na wszystkie dyski).

NT Advanced Serwer obsługuje także UPS oraz dokonuje automatycznej „odbudowy" utraconego połączenia klient/serwer.

Podsumowując, na polu bezpieczeństwa sieci WindowsNT wypada bardzo dobrze.

3.2. Exchange Server — elektroniczna wymiana dokumentów

Microsoft Exchange 5.0 [6] obsługuje wszystkie kluczowe protokoły internetowe, w tym POP3 dla dostępu do skrzynek pocztowych, SMTP do obsługi poczty elektronicznej, NNTP dla obsługi news'ów i list dyskusyjnych, LDAP dla dostępu do katalogów, HTML dla obsługi WWW i wreszcie SSL dla obsługi kwestii związanych z bezpieczeństwem.

Ważnym atutem Servera Exchange jest jego integracja z oprogramowaniem biurowym, na przykład z pakietem Office.

Exchange zapewnia kilka możliwości zabezpieczenia danych w protokole POP3. Dostępna jest prosta autentyfikacja jawnego tekstu, oraz architektura WindowsNT Challenge/Response zapewniająca bezpieczne logowanie się na serwerze. W połączeniu z autentyfikacją jawnego tekstu może być wykorzystany protokół SSL, co zapewnia szyfrowanie danych w kanale klient serwer.

Chociaż dostęp do LDAP nie jest chroniony hasłem, administratorzy mogą dokładnie określić te spośród atrybutów katalogów, które mają być widoczne dla nieuprzywilejowanych użytkowników. Można w ten sposób chronić informacje wewnętrzne, na przykład nazwisko kierownika lub numery telefonów.

Jak już wcześniej wspomniano, jednym z największych problemów związanych z siecią Internet jest bezpieczeństwo. Microsoft Exchange oferuje, w ramach protokołu SMTP, możliwość szyfrowania sesji pomiędzy hostami. W poprzedniej wersji (4.0) istniała możliwość wymiany zaszyfrowanych wiadomości w sposób zapewniający wysoki stopień bezpieczeństwa, ale nie dotyczyło to poczty przesyłanej poprzez Internet. W obecnej wersji można wymieniać klucze i certyfikaty bezpieczeństwa, również poprzez Internet. Użytkownicy mogą korzystać z usługi zaszyfrowanej, internetowej poczty elektronicznej.

Microsoft Exchange Server odznacza się dużą elastycznością dzięki tzw. modelowi pozwoleń. Model ten pozwala ustalać prawa dostępu i modyfikacji do poszczególnych kont użytkowników, pozwalając administratorom, na różnych poziomach, dzielić odpowiedzialność za system.

3.3. Serwer bazy danych

Bazy danych to zasadnicza część wielu systemów komputerowych. Przeważająca większość oprogramowania użytkowego jest oparta na systemach zarządzania bazami danych. W chwili obecnej odpowiedni poziom rozwoju i standaryzacji, umożliwiający komercyjne zastosowanie sieciowych systemów komputerowych, osiągnęły jedynie rozwiązania oparte na relacyjnych bazach danych i architekturze klient-serwer. Serwery relacyjnej bazy danych, pracujące w oparciu o język SQL, są najbardziej zalecaną technologią.

Sprawdzanie uprawnień do wykonania operacji na bazie danych przez serwer (a nie przez program użytkowy) zapewnia odporność na próby włamania z użyciem uniwersalnych narzędzi do edycji baz danych.

Oprócz tego serwery SQL oferują szeroką gamę usług, takich jak:

- dziennik transakcji,
- automatyczne tworzenie kopii bezpieczeństwa,
- informowanie administratora o awariach i błędach pracy serwera poprzez pocztę elektroniczną lub pager.

Jako serwer bazy danych został zarekomendowany Microsoft SQL Server, gdyż jest on zintegrowany z systemem operacyjnym Windows NT, posiada dobre parametry wydajnościowe i wbudowane mechanizmy ochrony.

3.4. Windows95

Systemy operacyjne sieci równorzędnych (peer-to-peer) nie są produktem szczególnie lubianym przez administratorów sieci komputerowych. Nie ma dla nich nic gorszego niż zorganizowani w grupę roboczą użytkownicy korzystający wspólnie z zasobów sieci, które co gorsza nie rezydują na jednym dedykowanym serwerze, ale porozrzucane są po wielu równorzędnych stacjach roboczych w sieci. Systemy te sprawdzają się jednak dobrze przy obsłudze sieci korporacyjnych. Poszczególne grupy użytkowników wolą eksploatować niewielki system i komunikować się z resztą firmy, na przykład przez serwer systemu NetWare.

Mechanizmy bezpieczeństwa, dostępne w systemie Windows95, chronią współdzielone zasoby sieci przed dostępem nieupoważnionych użytkowników. Użytkownicy mogą dzielić pliki i drukarki z innymi użytkownikami na dwóch poziomach. Innym użytkownikom systemu można nadać albo pełne prawa dostępu do katalogu, albo nadać im prawa tylko do odczytu plików bez możliwości ich modyfikacji. Dostęp nadawany jest poprzez przypisanie użytkownikom specyficznych haseł, związanych z odpowiadającym im poziomem zabezpieczenia. Podsumowując, w systemie Windows 95 ochrona danych jest właściwie scedowana na użytkownika.

4. Integracja sieci lokalnej z Internetem

Internet jest bezsprzecznie najbardziej efektywnym i opłacalnym sposobem połączenia telekomunikacyjnego pomiędzy odległymi miejscami. Pozwala na trwały transfer danych, dogodną komunikację z klientem, dostęp do odległych biur, zdalne zarządzanie rozproszonymi systemami, dostęp do danych bankowych czy choćby możliwość wykonywania pracy bez konieczności wychodzenia z domu (teleworking). Jedyną wadą jest brak wbudowanych mechanizmów ochrony, co w praktyce wyklucza wykorzystanie Internetu, w przypadku gdy wymagane jest stuprocentowe bezpieczeństwo przesyłania danych.

4.1. Zagrożenia

Użytkownik systemu komputerowego przyłączonego do sieci rozległej jest narażony na różnego rodzaju zagrożenia, jak:

- nieuprawnione monitorowanie danych (network monitoring) — technika ta polega na przechwytywaniu danych użytkownika zawierających między innymi takie dane, jak hasła, prywatną korespondencję, numery kart płatniczych czy inne dane;
- przechwytywanie połączeń (connection hijacking) — metoda ta pozwala na przejęcie już zainicjowanego połączenia i dołożenie dodatkowych poleceń, przy czym fakt ten nie musi być zauważony przez żadną ze stron, gdyż odpowiedzi systemu są filtrowane przed dojściem do prawowitego uczestnika sesji;
- przechwytywanie informacji routingowych (routing spoofing) — używane powszechnie protokoły routingowe oraz typowe ich konfiguracje pozwalają na nieuprawnione modyfikacje istniejących tablic routingu, narażając tym samym dane użytkowników na takie zagrożenia, jak przechwytywanie połączeń lub nieuprawnione monitorowanie danych;
- przechwytywanie pakietów komunikacji DNS (Domain Name Server spoofing) — jest to atak polegający na odsyłaniu spreparowanych pakietów UDP (protokół datagramów użytkownika) dla rozpropagowania nieprawdziwych informacji, które mogą być wykorzystane w przyszłości;
- atak typu odmowa usługi (denial of service attacks) — w najprostszym przypadku poprzez zasypywanie wskazanego serwisu lawiną pakietów atakujący uniemożliwia obsługę normalnych odwołań, a tym samym korzystanie z serwisu; atak ten ma najwięcej wysublimowanych form, może także być stosowany w połączeniu z atakami typu przechwytywanie informacji routingowych oraz przechwytywanie połączeń.

Zagrożenia są ogromne, a problem zabezpieczenia danych nie może być pozostawiony w rękach ich użytkowników. Zabezpieczenie dostępu do danych i zasobów sieciowych jest

problemem sieciowym! Administratorzy powinni dysponować narzędziami do kontroli dostępu zarówno z wewnątrz, jak i z zewnątrz sieci. Jest to konieczne do sprawowania nadzoru nad wykorzystaniem zasobów sieci i dostępu do danych. Oprócz monitorowania niezbędna jest także możliwość wprowadzenia ograniczeń dostępu i sterowania strumieniami informacji przepływającymi przez sieć. Podstawowych narzędzi, spełniających powyższe wymagania, dostarcza technologia pod nazwą Ściany Ogniowej (Firewall) [1].

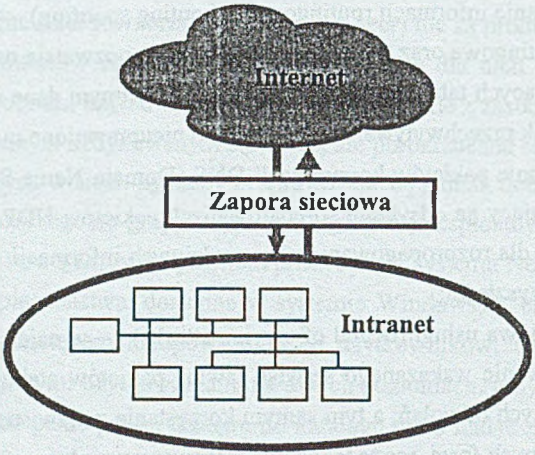
4.2. Firewall

Firewall (rys. 1) to komputer (zazwyczaj połączony routerami), który zostaje włączony pomiędzy sieć lokalną a sieć rozległą. Dobra konfiguracja Ściany Ogniowej wymaga, aby:

- cały ruch pomiędzy siecią lokalną a rozległą był kierowany przez Ścianę Ogniową,
- przechodził przez Ścianę Ogniową tylko ruch dozwolony,
- konfiguracja Ściany Ogniowej była odporna na ataki.

Zadaniami Ściany Ogniowej są:

- zabezpieczenie danych organizacji wewnątrz jej sieci lokalnej,
- kontrola dostępu do sieci lokalnej z zewnątrz,
- identyfikowanie i zapamiętywanie faktów uzyskania dostępu do sieci (auditing),
- natychmiastowe informowanie o próbach nieuprawnionych dostępów,
- zapewnienie ochrony danych zarówno opuszczających sieć, jak i danych do niej wpływających.



Rys. 1. Zapora sieciowa
Fig. 1.The Firewall

Najpopularniejsze rozwiązanie Ściany Ogniowej wykorzystuje jeden lub dwa routery (lub inne urządzenia dostępowe) oraz komputer (Firewall Host), który zajmuje się kontrolą komunikacji [1]. Rozwiązanie to jednak jest kosztowne ze względu na konieczność stosowania dodatkowego komputera (zazwyczaj pracującego pod kontrolą systemu UNIX), stosunkowo wolne (konieczne jest przepisywanie danych) oraz nie zabezpiecza skutecznie przed niektórymi sposobami ataku (na przykład przechwytywaniem informacji routingowych).

Innym popularnym sposobem jest wykorzystanie routerów wyposażonych w mechanizmy filtracji pakietów. Stosowanie nawet wielu filtrów pakietów nie powinno zwalniać prędkości urządzenia. Urządzenie powinno zapewniać filtrację wszystkich nagłówków pakietów, protokołu UDP (gopher, NFS), wszystkich wykorzystywanych protokołów komunikacyjnych (na przykład IP i IPX), a także umożliwiać zaawansowany auditing.

Czołowym dostawcą bezpiecznych routerów jest firma NSC (Network Systems Corporation) z Minneapolis. Rozwiązania NSC umożliwiają:

- stosowanie filtrów kompilowanych, a nie interpretowanych; w oczywisty sposób przyspiesza to proces filtrowania pakietów, pozwalając na stosowanie dużej liczby filtrów (nawet do 200, bez zauważalnego spadku prędkości),
- dynamiczne wprowadzanie nowych filtrów przy zauważonej próbie penetracji sieci,
- wykorzystywanie zaawansowanych mechanizmów auditingu,
- programowanie filtrów w języku wysokiego poziomu wraz z możliwością wykorzystywania dołączonej biblioteki,
- stosowanie Ściany Ogniowej dla protokołów różnych od IP.

Filtracja pakietów stosowana w routerach NSC opiera się na wykorzystywaniu informacji zawartej w poszczególnych warstwach sieciowych. Informacja zawarta w nagłówku pakietu jest wykorzystywana do określenia, czy pakiet powinien być dostarczony, czy datagram może być modyfikowany, czy i jak dane są zaszyfrowane oraz jakie są dopuszczalne drogi routingu. Ponadto, nagłówek jest wykorzystywany do prowadzenia statystyki.

Zgodnie z warstwową budową protokołów sieciowych, w różnych warstwach przesyłane są różne informacje. Daje to możliwość stosowania wielu filtrów.

Aby efektywnie korzystać z zawansowanych funkcji routera niezbędne są odpowiednie narzędzia dla administratorów sieci. NSC oferuje zestaw takich narzędzi pod nazwą Packet Control Facility (PCF). Pakiet składa się z kilku podstawowych części, realizujących następujące funkcje:

PCF Tools — narzędzia do tworzenia i zarządzania filtrami dla wszystkich routerów NSC,

PCF Logger — moduł notujący wszelkie próby naruszenia wprowadzonych zabezpieczeń, umożliwia konfigurację routera z konsoli poprzez UDP Console Logger oraz prowadzi statystykę wykorzystywania sieci przez poszczególne maszyny,

NetStalker — moduł wykrywający próby ataku oraz wszelkie niespodziewane zdarzenia w sieci.

Oprogramowanie PCF jest określane jako „Second Generation Firewalling". W porównaniu z obecnymi rozwiązaniami charakteryzuje go ogromne zwiększenie prędkości (50—100 razy w stosunku do Firewalls Hosts) oraz zmniejszenie kosztów instalacji (wymaga jednego routera, eliminuje potrzebę stosowania „Firewalls Hosts", a ponadto cena oprogramowania wliczona jest w cenę routera).

Bezpieczeństwo staje się typową usługą sieciową i może być stosowane dla sieci rozległych, jak i lokalnych, poprzez wprowadzenie Ścian Ogniowych pomiędzy poszczególnymi logicznymi segmentami sieci przedsiębiorstwa, na przykład Dział Księgowości lub Rozwoju Technicznego może być oddzielony od Wydziału Ewidencji Ludności. Zabezpiecza to sieć urzędu przed atakami wewnętrznymi, często groźniejszymi od ataków zewnętrznych.

Kontrola przesyłanej informacji to jednak jeszcze nie wszystko. Nawet jeżeli mamy pełną kontrolę nad przychodzącymi i wysyłanymi pakietami, to dane w nich zawarte są przesyłane w postaci jawnej. Umożliwia to „podsłuchiwanie" sieci, chociażby przy użyciu zaawansowanych analizatorów pakietów, i wykorzystanie otrzymanych w ten sposób danych, niezgodnie z ich przeznaczeniem, lub po prostu na zapoznanie się z tajnymi informacjami przez osoby niepowołane.

Publiczne sieci pakietowe są zazwyczaj o wiele ekonomiczniejsze w eksploatacji niż budowa własnej sieci rozległej opartej na liniach dzierżawionych. Linie takie zresztą wcale nie gwarantują bezpieczeństwa, ponieważ z reguły nie są nadzorowane i bardzo łatwo można uzyskać do nich dostęp (trasa ich przebiegu znana jest dużej liczbie osób). Jedynym dostępnym rozwiązaniem jest więc szyfrowanie przesyłanych danych. Routery NSC wykorzystują w tym celu zestaw programów zwanych wspólnie Data Privacy Facility (DPF). Oprogramowanie DPF spełnia następujące funkcje:

- **Prywatność** transmitowanych danych. Nie jest w praktyce możliwe odtworzenie zawartości przesyłanego komunikatu, nawet poprzez szczegółową analizę zarejestrowanego strumienia danych.
- **Autentyczność**. Potwierdza fakt dotarcia transmisji do źródła przeznaczenia oraz to, że transmisja dotarła z uprawnionego źródła, a nie została wprowadzona do sieci przez zdolnego hackera.
- **Odpowiedzialność**. Osoba, która stworzyła dane i przekazała je do transmisji, nie może się wyprzeć tego faktu.

Oprogramowanie PDF może wykorzystywać następujące algorytmy szyfrujące:

- IDEA — International Data Encryption Algorithm,
- DES — Data Encryption Standard,

- NSC1 — Network Systems Cipher#1.

Autentyczność, kompresję oraz przekazywanie klucza zapewniają:

- MD5 — standard podpisu elektronicznego,
- ALDC — Adaptive Lossless Data Compression (licencja IBM),
- Diffie — Hellman Key Exchange,
- RSA Key Authentication — 512- lub 1024-bitowe klucze prywatne lub publiczne.

Poszczególne funkcje PDF mogą być konfigurowane w miarę potrzeb. I tak na przykład:

- dane utajniane wymagają prywatności; zapewnia to szyfrowanie przesyłanych danych,
- wszystkie programy powinny sprawdzać autentyczność danych,
- dane o faktycznym nadawcy i odbiorcy są zawarte w utajnionej (zaszyfrowanej) części pakietu i opatrzone podpisem elektronicznym,
- dane przesyłane w celu zarządzania siecią, programy routerów oraz transakcje powinny kontrolować integralność danych,
- oprogramowanie PDF sprawdza, czy treść otrzymanego pakietu nie została zmieniona, na przykład poprzez planowaną ingerencję w trakcie jego transmisji,
- zabezpieczenie przed powtórnym użyciem, już wykorzystanych danych, powinno być regułą dla wszystkich aplikacji, co uniemożliwia ewentualne, powtórne wykorzystanie przechwyconego pakietu w niecnych celach.

Omówione mechanizmy zabezpieczeń pozwalają na zabezpieczenie sieci urzędu przed atakiem z zewnątrz, z zachowaniem swobodnego dostępu do sieci Internet, oraz na wykorzystanie sieci Internet jako medium transmisyjnego do przesyłania danych pomiędzy centralą a oddziałami na całym świecie, z równoczesnym zachowaniem ich poufności.

NSC oferuje trzy typy bezpiecznych routerów, z których każdy wyposażono w omówione powyżej zabezpieczenia. Są to:

- **NSC BorderGuard router**; 1 port LAN, do trzech portów WAN (X.21, RS23, RS449 itp. do wyboru). Urządzenie to typowy router/bridge przeznaczony do realizacji bezpiecznego dostępu do sieci lokalnej lub rozległej. Jest on wyposażony w oprogramowanie PCF i PDF; został wybrany przez firmę Hawlett-Packard jako rozwiązanie Firewall dla serwerów WWW.
- **NSC Security router;** 4 porty LAN/WAN w różnych konfiguracjach z FDDI (jedno- i wielomodowym) włącznie, może być zaliczony do kategorii „średnich" i stosowany w dużych, bezpiecznych instalacjach do komunikowania grup użytkowników zabezpieczonych zarówno przed atakiem z zewnątrz, jak i wewnątrz. Wyróżniony nagrodą „BEST OF SHOW" przez Data Communications i LAN Times podczas wystawy NetWord+Interop w Las Vegas w 1995 roku.

– **NSC Enterprise Router/Swich (ERS).** Zaawansowany modułowy „backbone route/switch". Przeznaczony do bardzo dużych i „odpowiedzialnych" instalacji. Obejmuje wszystkie interfejsy z HSSI i ATM (OC-3 i DS3) włącznie. Prędkość ponad 500000 pps, switch latency time < 0,6 us. Wyposażony w zaawansowane mechanizmy zabezpieczenia przed awarią (redundantne zasilacze, procesory, interfejsy itp. oraz dyski twarde).

Warto też wspomnieć o innym rozwiązaniu problemów związanych z poufnością, bezpieczną komunikacją i integralnością danych użytkownika sieci rozległej. Rozwiązaniem takim jest SSH (Secure Shell) — protokół zapewniający bezpieczne połączenie typu login, X11, dostęp terminalowy do komputerów w sieci TCP/IP, a także bezpieczny transfer plików.

Protokół SSH wykorzystuje kryptograficzne uwierzytelnianie, automatyczne szyfrowanie sesji oraz zapewnia integralność przesyłanych danych. Posługuje się algorytmem RSA do wymiany kluczy w procesie uwierzytelniania oraz używa symetrycznych algorytmów, takich jak IDEA lub potrójny DES do szyfrowania sesji użytkownika.

SSH jest protokołem pakietowym pracującym na dowolnej warstwie transportowej, pozwalającej na przesłanie binarnego strumienia danych. Typowo do tego celu wykorzystywany jest TCP/IP. Obecna implementacja pozwala ponadto na użycie dowolnego programu zastępczego do komunikacji z serwerem, zawiera także mechanizmy obsługi SOCKS i Firewall FWTK (Trusted Information Systems) [7].

5. Podsumowanie

Modernizacja systemu zarządzania w Urzędzie Miasta Pszów obejmuje wielokierunkowe działania, do których należą:

- wdrożenie oprogramowania użytkowego w jednostkach nie dysponujących obecnie wspomaganiem komputerowym,
- rozpoczęcie realizacji systemu informacji o terenie (GIS),
- integracja i współdziałanie istniejących systemów (baz danych),
- wprowadzenie w szerokim zakresie elektronicznego obiegu dokumentów,
- wprowadzenie systemu obsługi pracowników,
- zrealizowanie systemu wymiany informacji z jednostkami podrzędnymi,
- dostęp do sieci Internet i komunikacja z jednostkami nadrzędnymi,
- zwiększenie bezpieczeństwa danych i kontroli dostępu do baz danych,
- stworzenie telefonicznego systemu informacji o urzędzie i mieście.

Na ile wskazane rozwiązania okażą się skuteczne, pokaże życie. Wydaje się jednak, iż próba połączenia lokalnych systemów zarządzania z systemami wojewódzkimi i krajowymi przy wykorzystaniu sieci Internet jest celowa i możliwa do realizacji.

LITERATURA

[1] Garfinkel S., Spafford G.: Bezpieczeństwo w Unixie i Internecie. Wydawnictwo RM, Warszawa 1997.

[2] Grzywak A., Kozielski S., Nałęcki K., Lorek M., Koncepcja zmodernizowania systemu zarządzania Urzędem Miasta Pszów z uwzględnieniem połączenia systemów lokalnych z systemami wojewódzkimi i krajowymi. Politechnika Śląska Instytut Informatyki, Gliwice, maj 1997.

[3] Hryń G., Cieśla S.: Metody zapewnienia bezpieczeństwa w systemie Windows NT. Zeszyty Naukowe Politechniki Ślaskiej, seria Informatyka, z. 32, 1997, s. 215—228.

[4] Nałęcki K.: Intranet — metodyka, środki, zastosowania. Zeszyty Naukowe Politechniki Ślaskiej, seria Informatyka, z. 32, 1997, s. 379—399.

[5] Sheldon T.: WindowsNT struktura i użytkowanie. Wydawnictwo Robomatic, Wrocław, 1994.

[6] Microsoft Exchange. Microsoft Corporation 1997.

[7] Network Systems Corporation. Materiały firmowe 1997.

Recenzent: Dr hab. inż. Adam Mrózek, Prof. Politechniki Śląskiej

Wpłynęło do Redakcji 6 stycznia 1998 r.

Abstract

Paper is devoted to problems of security of resources in a large multimedia information exchange system, with special accent given to the problems of building and integration of local area networks and connecting them to Internet. Methods for security of resources against external as well as internal attacks are presented.

An assumption has been made that the system is to be an everyday-use tool for communication between the municipal office employees, with Internet access for those who need it. As

seen from outside, the system should serve wide variety of information services for both the office clients and city inhabitants, as well as it should promote the city.

To satisfy these assumptions, it seems to be suitable to implement the same technologies and tools for both Internet services and local area network (intranet). This covers e-mail, news boards, applications based on Web technologies and data bases.

Paragraph 2 presents the security strategy accepted for the system, which is a compromise between a system fully secure (which cannot be open), and a system well integrated with Internet. Taking into account this strategy, as well as general assumptions accepted for the system, a Microsoft Network solution has been proposed, with Windows NT/95-based workstations. In paragraph 3 proposed software solutions have been described in brief (WindowsNT, Exchange Server, SQL Serwer, Windows 95).

Paragraph 4 presents problems of integration local area networks with Internet, with accent given to the dangers of such integration and methods for securing the system. In particular, Firewall technology has been proposed as the main security means.

The solutions proposed in the paper are being implemented in municipal office of the city of Pszów.