BIULETYN INFORMACYJNY INSTYTUTU ŁĄCZNOŚCI

1997
8

BIULETYN INFORMACYJNY INSTYTUTU ŁĄCZNOŚCI

ROK 37 INSTYTUT ŁĄCZNOŚCI NR 8(353)

WARSZAWA 1997

ISSN 0209-1046

Redaktor: mgr Krystyna Juszkiewicz

Skład komputerowy: Barbara Skwara

Instytut Łączności, Ośrodek Informacji Naukowej i Normalizacji
ul. Szachowa 1, 04-894 Warszawa

Elżbieta Andrukiewicz

SIECI LOKALNE - ZAGROŻENIA, SŁABOŚCI, ZABEZPIECZENIA

SPIS TREŚCI

Elżbieta Andrukiewicz

621.395.743

SIECI LOKALNE - ZAGROŻENIA, SŁABOŚCI, ZABEZPIECZENIA

1. WSTĘP

Sieci lokalne *(LAN - Local Area Networks)* stają się środkiem realizacji potrzeb organizacyjnych i komunikacyjnych w coraz większej liczbie przedsiębiorstw. W informatycznej epoce poprzedzającej stosowanie sieci lokalnych większość procesów obliczeniowych i komunikacyjnych było realizowanych centralnie; również zarządzanie informacją i jej zabezpieczeniem odbywało się w ten sposób. Ideą sieci lokalnych jest rozproszenie przetwarzania danych. W konsekwencji, także funkcje komunikacji są rozproszone w całym przedsiębiorstwie. W ślad za rozproszeniem usług sieciowych, również usługi zabezpieczenia związane z przechowywaniem, przetwarzaniem i przesyłaniem danych muszą zostać rozproszone. Przykładowo, wysłanie za pośrednictwem sieci LAN poufnych plików z jednego systemu, w którym są one chronione mechanizmami kontroli dostępu do drugiego systemu, w którym zabezpieczeń w postaci kontroli dostępu nie ma, niweczy wysiłki i nakłady poniesione w pierwszym systemie. Użytkownik musi mieć pewność, że jego dane oraz sama sieć są dostatecznie zabezpieczone.

Bezpieczeństwo sieci lokalnych przez długi czas nie było przedmiotem uwagi producentów sprzętu, programistów oraz właścicieli i użytkowników tych sieci. Owszem, panowała opinia, że sieć rozległa (Internet) jest źródłem wszelkiego zła, natomiast sieć lokalna to środowisko przyjazne i bezpieczne. Opinia taka była podtrzymywana zwłaszcza przez producentów sprzętu i oprogramowania, którzy w reklamach swoich produktów nacisk kładli (i w dalszym ciągu kładą) na zalety użytkowe, a pomijali całkowicie aspekt zabezpieczenia sieci.

Należy odnotować brak całościowych opracowań tej tematyki, zarówno w kraju, jak i za granicą. Konsekwencją pomijania problematyki zabezpieczenia sieci lokalnej jest zastraszający wskaźnik rejestrowanych przypadków włamań do sieci lokalnych, utrata poufnych danych, straty przedsiębiorstw itp. (por. pkt 1.2).

Gwałtowny rozwój sieci lokalnych, szeroki zakres nowych zastosowań, ostra konkurencja miedzy producentami sprzętu i oprogramowania sieciowego przy jednoczesnym wzroście uzależnienia przedsiębiorstw od sieci lokalnych powodują, że problem zabezpieczenia tych sieci nabiera szczególnego znaczenia. W tym artykule przedstawiono zagrożenia, na jakie jest narażona sieć lokalna, słabości sieci, które powodują, że prawdopodobieństwo naruszenia jej zabezpieczenia jest realne oraz mechanizmy zabezpieczeń specyficzne dla sieci lokalnej.

1.1. Cele zabezpieczenia sieci lokalnej

Zabezpieczenie sieci lokalnej wymaga spełnienia następujących kryteriów:

- **poufności** danych składowanych, przetwarzanych i transmitowanych w sieci LAN;
- **integralności** danych składowanych, przetwarzanych i transmitowanych w sieci LAN;
- **dostępności** danych i zasobów LAN, a także zdolności systemu do przetwarzania oraz transmitowania informacji z zachowaniem sieciowych wymagań czasowych.

Te trzy kryteria zostały użyte w definicji zabezpieczenia systemu informatycznego w normie brytyjskiej [5] i standardzie amerykańskim [8].

Rozwój sieci lokalnych w kierunku systemów rozproszonych spowodował konieczność uzupełnienia powyższej definicji. System informatyczny w przedsiębiorstwie (czyli, po prostu, sieć lokalna) powoli przestaje być traktowany jako forteca, w której stosowane mecha-

nizmy szyfrowania, fizycznego wydzielenia i kontroli dostępu służą wyłącznie ochronie informacji przed nieupoważnionym dostępem. Taki sposób ochrony jest niezwykle kosztowny i trudny w utrzymaniu [19]. Często zdarzało się w przeszłości, że zabezpieczenie sieci było naruszane przez zastosowanie prostych mechanizmów, wykorzystujących luki w systemie. W definicji zabezpieczenia sieci dodano zatem dodatkowe kryteria kontrolne zapewnienia:

- **możliwości ewidencjonowania (rozliczalności)** działań podejmowanych w sieci LAN;
- **autentyczności (uwierzytelniania)** użytkowników i zasobów sieci LAN.

Ostatnio [15] dodano jeszcze jedno, szóste kryterium - **niezawodności** (*reliability*). Przez to rozumie się gwarancję spójnego i zgodnego z zamierzeniami zachowania się sieci LAN oraz przetwarzanych danych.

Zabezpieczenie systemów informatycznych obejmuje wszelkie działania związane ze zdefiniowaniem, osiągnięciem i utrzymaniem celów zabezpieczenia, jakimi są: poufność, integralność, dostępność, możliwość ewidencjonowania, uwierzytelnianie i niezawodność. Omówienie zależności między poszczególnymi elementami systemu zabezpieczeń i dynamicznego charakteru tych zależności można znaleźć w [1]. W niniejszym artykule skoncentrowano się na sieci lokalnej i specyficznych dla niej problemach zabezpieczenia.

1.2. Problem naruszania zabezpieczeń

Przez **naruszenie** zabezpieczeń należy rozumieć taką zmianę stanu systemu informatycznego, w którym co najmniej jedno z wymienionych w poprzednim punkcie kryteriów nie jest spełnione. Przy analizie problemu zabezpieczeń należy wziąć pod uwagę trzy fakty, które wynikają z badań prowadzonych w ciągu ostatnich kilku lat:

- większość naruszeń zabezpieczeń przechodzi nie zauważona,
- większość zauważonych naruszeń zabezpieczeń nie jest raportowana,
- zagrożenia zewnętrzne są realne, jednakże większość naruszeń ma swe źródło wewnątrz przedsiębiorstwa, a nie poza nim.

Jaka jest proporcja między zewnętrznymi a wewnętrznymi źródłami naruszeń? Prowadzone badania, które mogą dać odpowiedź na to pytanie, są obarczone wysokim marginesem błędów. Przedsiębiorstwa niechętnie ujawniają swoje tajemnice. Niemniej jednak, można spotkać przybliżone oszacowania. W [6] podano, że ponad 90% naruszeń zabezpieczeń ma swą przyczynę wewnątrz systemu. Inne źródło [9] utrzymuje, że za 85% zdarzeń, które można uznać za atak na system informatyczny, odpowiedzialność ponoszą pracownicy przedsiębiorstwa. Jeszcze inne źródła podają następujący rozkład odpowiedzialności: 40% - z zewnątrz, 40% - z wewnątrz, a pozostałe 20% - to łączny wysiłek "intruzów" zewnętrznych i wewnętrznych. Pewną ogólną tendencję można jednak zdefiniować następująco. **Niezależnie od tego, czy sieć lokalna ma połączenie z zewnętrzną siecią rozległą czy też nie, główne źródło naruszeń zabezpieczeń tkwi w niej samej. Należy zatem główną uwagę poświęcić sieci lokalnej, a nie jej otoczeniu.**

2. FUNKCJE I STRUKTURA SIECI LOKALNEJ

2.1. Definicja LAN

Zgodnie z definicją podaną przez IEEE (*Institute of Electrical and Electronic Engineers),* sieć lokalna jest "systemem transmisji danych umożliwiającym bezpośrednią komunikację między pewną skończoną liczbą niezależnych urządzeń, działającym na ograniczonym, w sensie geograficznym, obszarze i wykorzystującym fizyczne kanały komunikacyjne o średnich przepustowościach" [8]. Zwykle LAN jest własno-

ścią lokalnego operatora, nie związanego z operatorem publicznym. Sieć lokalna działa pod wspólnym systemem operacyjnym, łącząc serwery, stacje robocze i urządzenia magazynowania danych oraz umożliwiając użytkownikom wspólne wykorzystywanie zasobów i funkcji oferowanych przez tę sieć.

2.2. Funkcje tradycyjnej sieci lokalnej

- **Rozproszone składowanie plików**

Funkcja rozproszonego składowania plików umożliwia użytkownikom dostęp do danych magazynowanych na odległym serwerze. Funkcja rozproszonego składowania plików obejmuje zdalne:
- operacje na plikach: dostęp, odczyt i zapis,
- drukowanie.

- **Zdalne przetwarzanie**

Zdalne przetwarzanie polega na uruchomieniu jednej lub kilku aplikacji na odległym serwerze. Zdalne przetwarzanie pozwala na zdalne:
- zarejestrowanie się *(login)* w innym serwerze LAN,
- wykonanie aplikacji rezydującej w innym serwerze LAN,
- uruchomienie aplikacji w jednym lub kilku serwerach LAN

tak, jakby użytkownik wykonywał powyższe działania lokalnie.

- **Przesyłanie wiadomości**

Przesyłanie wiadomości w sieci LAN realizują usługi: poczty elektronicznej i konferencji. Poczta elektroniczna jest oferowana przez większość sieci LAN i powoli zastępuje zwykłe procedury komunikacji wewnętrznej oraz zewnętrznej przedsiębiorstw. Serwery poczty

elektronicznej działają podobnie jak zwykłe lokalne placówki pocztowe, umożliwiając użytkownikom nadawanie i odbiór wiadomości przesyłanych za pośrednictwem sieci LAN. Konferencja jest realizowana w sieci podobnie jak w telefonii analogowej.

2.3. Nowe zastosowania sieci lokalnych - nowa generacja sieci lokalnych

W ostatnich latach nastąpiły duże zmiany na rynku usług teleinformatycznych. Obecnie do głównych kierunków rozwoju teleinformatyki należy zaliczyć:

- rozwój techniczny i technologiczny telekomunikacji, zwiększający szybkości przepływu informacji przy jednoczesnym gwałtownym spadku cen urządzeń;
- stale rosnące możliwości obliczeniowe mikroprocesorów przy jednoczesnym spadku kosztu jednostkowego przetwarzania informacji;
- rozwój nowych technik masowego przechowywania danych, w tym dysków optycznych: skracanie czasu dostępu do informacji i zmniejszanie kosztów jej przechowywania;
- gwałtowny rozwój Internetu, otwierajacy możliwość łączenia sieci lokalnych za pośrednictwem ogólnoświatowej sieci rozległej;
- dynamiczny rozwój nowych usług opartych na przetwarzaniu informacji w środowisku graficznym;
- powstawanie multimedialnych baz danych.

Rozwój sieci lokalnych podąża za wyżej przedstawionymi kierunkami rozwoju całej dziedziny przetwarzania i przesyłania informacji. Wprowadzenie do sieci lokalnych nowych zastosowań opartych na przetwarzaniu informacji graficznych, możliwość dostępu do multimedialnych informacji gromadzonych w Internecie, wykorzystywanie narzędzi tworzenia i zarządzania multimedialnymi bazami danych otwierają przed przedsiębiorstwani nowe obszary zastosowań swoich sieci komputerowych. Jednocześnie, te nowe zastosowania wymagają

zmian w topologii sieci i technice urządzeń sieciowych. Aby sprostać konkurencji, wiele przedsiębiorstw musi podjąć decyzję o gruntownym unowocześnieniu swoich sieci tak, aby mogły one podołać nowym wymaganiom w zakresie szybkości przetwarzania danych i przepustowości połączeń sieciowych. W poniższych tablicach przedstawiono przykładowe wymagania na składowanie (tabl. 1) i przesyłanie (tabl. 2) informacji graficznych.

Tablica 1

Konwersja dokumentów na pliki postaci graficznej

Typ dokumentu	Rozdzielczość	Wielkość ramki [bity]	Wielkość pliku (bez kompresji) [MB]	Współczynnik kompresji
Czarno-biały - o niskiej rozdzielczości (np. fax G3)	200x100 dpi	1700x1200x1 (A4 = 8,5"x12"x1)	0,25	od 10:1 do 15:1
Czarno-biały o wysokiej rozdzielczości (np. rysunek techniczny)	300x300 dpi	2550x3600x1 (A4 = 8,5"x12"x1)	1,15	20:1
Kolorowy obraz o niskiej rozdzielczości	640x480 punktów	640x480x24	0,92	20:1
Kolorowy obraz o wysokiej rozdzielczości	1024x768 punktów	1024x768x24	2,36	30:1
Obraz z ultrasonografu	128 x128 punktów	128x128x8	0,016	2,5:1
Fotografia rentgenowska	1024x1024 punkty	1024x1024x12	1,57	2,5:1
Fotografia w profesjonalnych zastosowaniach	1000x1000 dpi	8500x12000x24 (A4 = 8,5"x12"x24)	306	20:1

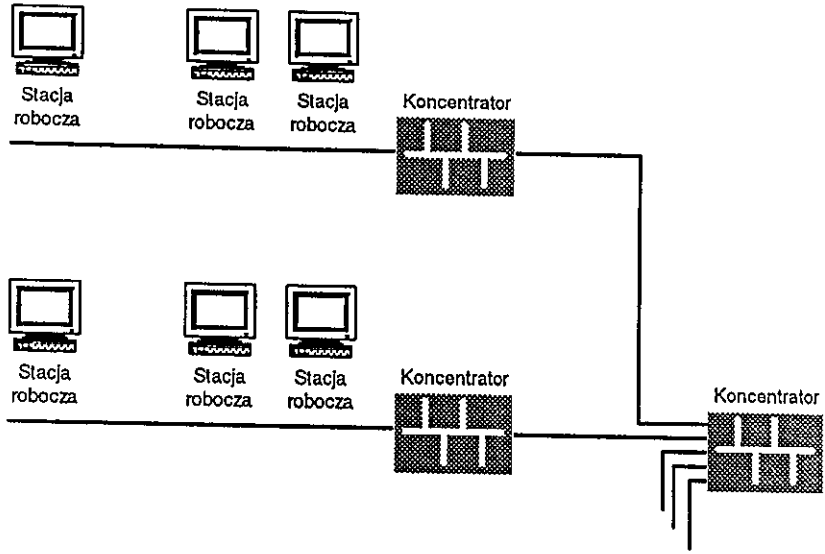
Tablica 2

Transmisja informacji graficznej w sieciach komputerowych

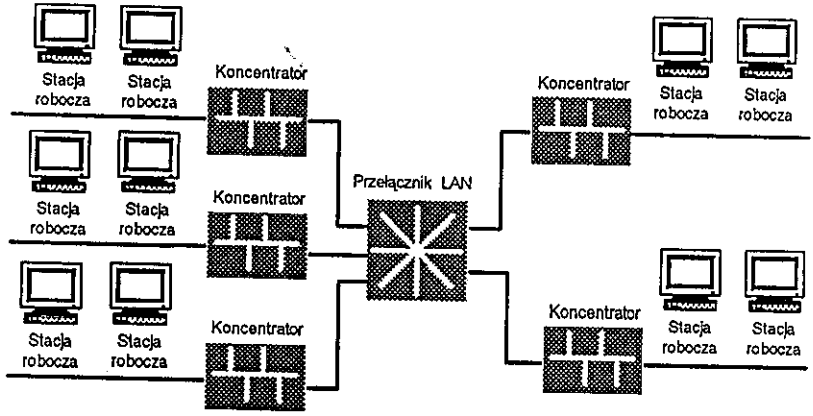
Typ zastosowania	Metoda kompresji	Wymagana przepustowość na 1 użytkownika sieci
Wideokonferencja	ITU-T H.320	128-768 kbit/s
Multimedialne aplikacje	Intel Indeo®	64 kbit/s - 400 kbit/s
Filmy i usługi zdalnego nauczania	MPEG-1 (MPEG-2)	1,5 (6) Mbit/s
Telewizja wysokiej rozdzielczości (HDTV)	AT&T/Zenith	21 Mbit/s

Jak wynika z tych tablic, tradycyjne sieci lokalne, zarówno pod względem topologii, mocy przetwarzania serwerów i stacji roboczych, jak i realizowanych protokołów, nie są w stanie podołać nowym wymaganiom. Sieci te, budowane w latach osiemdziesiatych, były realizowane głównie w technice Ethernet lub Token Ring. Całkowita przepustowość takich sieci wynosiła, odpowiednio, 10 Mbit/s oraz 4/16 Mbit/s. Przepustowość przypadająca na jednego użytkownika sieci wynikała z podzielenia przepustowości całkowitej przez liczbę użytkowników sieci (rys. 1). Aby sprostać nowym potrzebom komunikacyjnym użytkowników, należy budować sieci lokalne nowej generacji. Przykład ewolucji struktury sieci lokalnych w kierunku uzyskania większych przepustowości przy częściowym wykorzystaniu struktury istniejącej przedstawiono na rys. 2. Szerokie omówienie zmian zachodzących w sieciach lokalnych w ostatnich latach można znaleźć w [16].

Nowe zastosowania sieci wymuszają nową organizację pracy w przedsiębiorstwie. Wymagają określania zamkniętych grup roboczych, obiegu i dzielenia obiektów (dokumentów, wykresów, tabel,



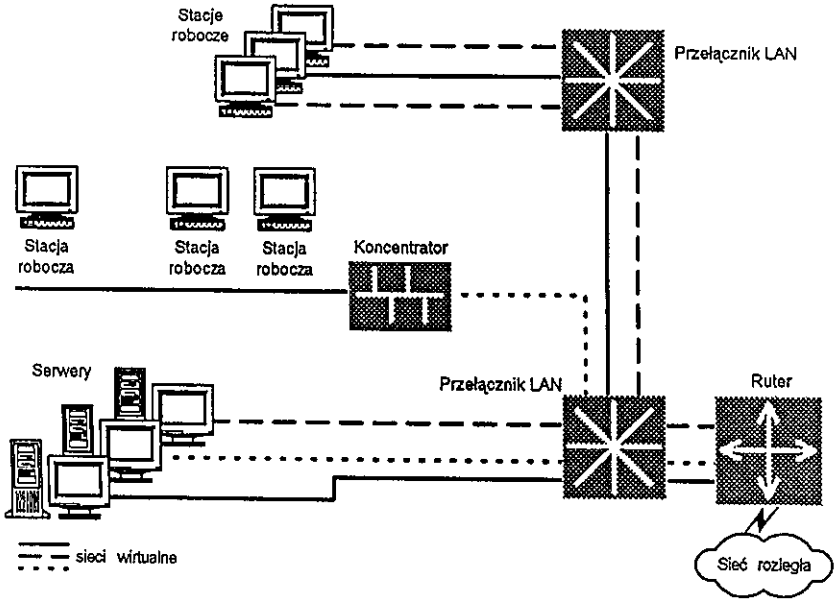
Rys. 1. Lokalna sieć w układzie tradycyjnym, jednosegmentowym: przepustowość całkowita = 10 Mbit/s, 100 użytkowników ⇒ 100 kbit/s na 1 użytkownika



Rys. 2. Lokalna sieć pięciosegmentowa o zwiększonej przepustowości: przepustowość całkowita = 50 Mbit/s, 5 grup x 20 użytkowników ⇒ 500 kbit/s na 1 użytkownika

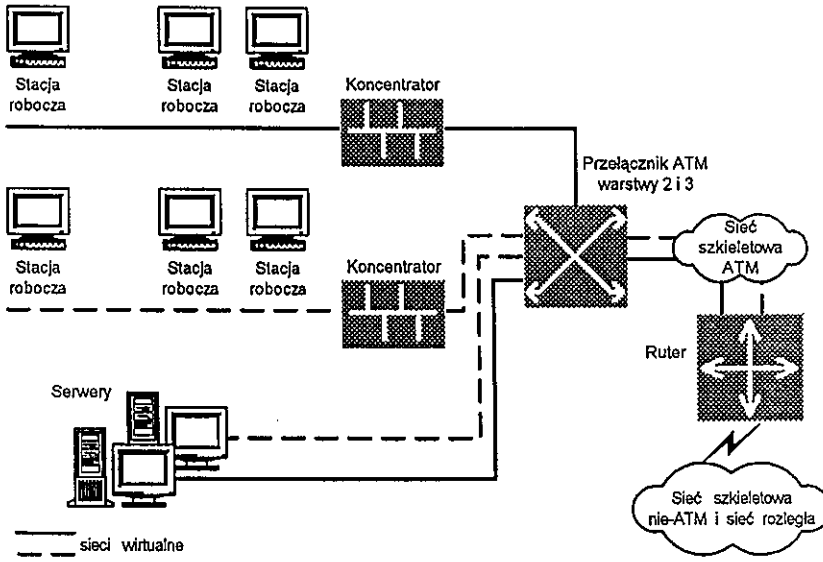
obrazów), sposobów wykorzystania poczty grupowej i wideokonferencji. W dużej swej części korzystają z koncepcji Intranetu - sieci lokalnej zbudowanej z uwzględnieniem mechanizmów stosowanych w sieci globalnej Internet. Sieć lokalna musi zatem odpowiadać nowym wymaganiom pod względem topologii, przepustowości i stosowanych protokołów.

Na rys. 3 i 4 przedstawiono poglądowe konfiguracje sieci lokalnych, wykorzystujące nowe topologie (segmentacja sieci, sieci wirtualne) i nowe technologie (ATM).



Rys. 3. Koncepcja sieci wirtualnych z zastosowaniem techniki Ethernet/Fast Ethernet [3]

Jaki wpływ na bezpieczeństwo sieci mają nowe techniki, topologie i protokoły? Problem ten zostanie omówiony w pkt. 3.5 i 3.6.



Rys. 4. Koncepcja sieci wirtualnych przy użyciu techniki ATM [3]

3. PROBLEMY ZABEZPIECZENIA SIECI LOKALNEJ

3.1. Rozproszone składowanie plików

Serwery realizujące funkcje składowania plików umożliwiają kontrolę dostępu użytkownika do różnych obszarów ich magazynowania. Jest ona zwykle oparta na zezwoleniu użytkownikowi na dostęp do określonych katalogów i użytkowania na zasadzie lokalnego dysku. Mogą pojawić się tutaj dwa problemy. Po pierwsze, serwer może gwarantować kontrolę dostępu na poziomie katalogu, tak więc użytkownik, mając zezwolenie na dostęp do katalogu, uzyskuje też dostęp do wszystkich zawartych tam plików. Aby zminimalizować ryzyko powstania takiej sytuacji, należy ze szczególną starannością zaprojek-

tować właściwą strukturę systemu składowania plików oraz zapewnić właściwe zarządzanie tym systemem. Drugi problem pojawia się w przypadku niewystarczających mechanizmów zabezpieczeń istniejących na lokalnej stacji roboczej. Przykładowo, przechowywana na komputerze PC informacja nie jest w żaden sposób zabezpieczona. Kopiując plik z serwera na lokalny dysk komputera PC, użytkownik traci zabezpieczenie tego pliku. Jeśli taka sytuacja jest niedopuszczalna, należy rozważyć zagadnienie wprowadzenia zabezpieczeń w środowisku komputerów osobistych.

3.2. Zdalne przetwarzanie

Sieć lokalna powinna zapewnić autoryzowany dostęp do odległych urządzeń i zdalnych usług. Serwery muszą być zdolne do uwierzytelnienia użytkowników żądających dostępu do usług lub aplikacji. Z drugiej strony, użytkownicy muszą mieć pewność uwierzytelnienia lokalnych i zdalnych serwerów. Nieprawidłowy mechanizm uwierzytelnienia może prowadzić do nieupoważnionego dostępu do serwerów i aplikacji. Ponadto, musi istnieć mechanizm kontroli integralności aplikacji wykorzystywanych przez wielu użytkowników sieci LAN.

3.3. Przesyłanie wiadomości

Niedostateczna ochrona poczty elektronicznej umożliwia przejęcie, zmianę treści i retransmisję przechowywanych lub przesyłanych wiadomości, powodując utratę ich poufności i integralności. Z przesyłaniem wiadomości łączy się także problem dostępu do nich spoza sieci lokalnej.

3.4. Zdalny dostęp

Zwiększa się liczba osób, których praca jest związana z dostępem do zasobów sieci loklanej niezależnie od miejsca, w którym się znajdują. Osobom takim należy zapewnić:

- dostęp do zasobów sieci, zgodnie z przywilejami, jakie im przyporządkowano jako użytkownikom, za pośrednictwem mechanizmu uwierzytelnienia, zarówno użytkownika, jak i sieci;
- integralność i poufność przesyłanych wiadomości.

Pojawia się zatem problem dołączenia struktury sieci lokalnej do systemu telekomunikacyjnego przedsiębiorstwa - jego centrali abonenckiej, zainstalowania modemów i ich zintegrowania z siecią lokalną.

3.5. Topologie i protokoły

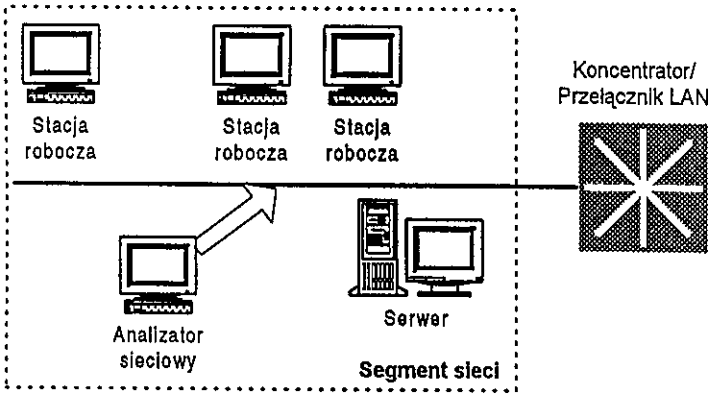
Topologia i protokoły sieci lokalnych są logiczną konsekwencją pierwotnych założeń przyświecających koncepcji sieci lokalnej: prostoty struktury, efektywności działania i niskiego kosztu transmisji. Niezależnie od rozwoju technik realizacji sieci lokalnych - wprowadzenia okablowania strukturalnego, segmentacji sieci, szybkich mostów i przełączników - nie zmieniła się natura sieci eternetowej. Rozgłaszanie (*broadcasting*) powoduje, że ruch transmitowany w sieci musi przejść przez wszystkie stacje dołączone do danego segmentu sieci.

Protokoły sieciowe - IP, Novell IPX, Lan Manager - opierają się na wirtualnych, a nie fizycznych połączeniach między węzłami sieci, jako metody tańszej i prostszej do utrzymania. Wirtualne połączenia wymagają dostępności przesyłanych wiadomości w wielu węzłach pośrednich. Zatem, nie tylko sama topologia sieci oraz natura sieci LAN (rozgłaszanie), ale także stosowane protokoły powodują, że pakiety są dostępne w kolejnych pośrednich węzłach sieci oraz krążą między segmentami.

Z natury sieci LAN i przyjętych protokołów wynika niebezpieczeństwo podsłuchu, aktywnego lub pasywnego. Pasywny podsłuch obejmuje nie tylko rejestrowanie przesyłanych informacji, ale także prowadzenie analizy ruchu w sieci: wykorzystywania adresów, innych danych znajdujących się w nagłówkach, długości wiadomości i czę-

stości ich przesyłania. Aktywny podsłuch oznacza próbę modyfikacji strumienia przesyłanych danych: zmianę, opóźnienie, powielenie, usunięcie lub zniekształcenie przesyłanych wiadomości.

Analizator sieciowy - narzędzie niezbędne w pracy administratorów sieci - włączony do sieci przez intruza umożliwia przechwytywanie i analizę ruchu. Oprogramowanie zmieniające standardowy komputer PC386, wyposażony w kartę sieciową, w analizator ruchu jest publicznie dostępne. Na rys. 5 przedstawiono możliwość analizy ruchu w danym segmencie sieci lokalnej.



Rys. 5. Możliwość analizy ruchu sieciowego w segmencie LAN

Nowe zastosowania, omówione w pkt. 2.3, spowodowały szybki rozwój aplikacji opartych na protokole TCP/IP i wykorzystujących koncepcję adresowania identyczną do stosowanej w Internecie. Wprowadzenie do sieci lokalnych Intranetu - to wpuszczenie "dżina internetowego" do przyjaznego środowiska sieci lokalnej. W sieci lokalnej nie ma urządzeń zabezpieczających przed zagrożeniami wynikającymi ze struktury protokołu TCP/IP- nie ma ruterów w węzłach pośrednich i "zapór ogniowych" *(firewalls)*. W rezultacie, sieć lokalna może zostać narażona na wszystkie zagrożenia i ataki poznane oraz praktykowane w ciągu kilkunastu lat rozwoju Internetu.

Zastraszające wskaźniki naruszeń zabezpieczeń sieci lokalnych mogą przybrać jeszcze gorszą postać, jeśli do sieci lokalnych nie wprowadzi się odpowiednich mechanizmów zabezpieczeń przed zagrożeniami intranetowymi.

W pkt. 5 zostaną przedstawione mechanizmy minimalizujące ryzyko związane ze słabościami protokołu TCP/IP, zagrożeniami ataku za pomocą metod znanych z Internetu oraz sposoby kontrolowania urządzeń sieciowych.

3.6. Zarządzanie siecią

Problem **zarządzania siecią** staje się kluczowy wobec nowych zagrożeń, opisanych poprzednio. Zintegrowane, centralne systemy zarządzania sieciami lokalnymi są bardzo kosztowne, zatem mało przedsiębiorstw stać na ich instalację, a jeśli nawet, to rzadko wykorzystują w pełni ich możliwości. Ponadto, często zdarza się, że poszczególne elementy sieci (koncentratory, przełączniki) mają niekompatybilne moduły zarządzania, trzeba więc zarządzać nimi autonomicznie i lokalnie.

Problem zarządzania jest szczególnie dotkliwy w przypadku nowoczesnych urządzeń sieciowych opartych na technice ATM. Nad standaryzacją protokołów związanych z adaptacją ATM do stosowania w sieciach lokalnych ciągle trwają prace. Główny kierunek działań zespołów standaryzacyjnych to uzgodnienie interfejsów i protokołów, a nie zagadnienia bezpieczeństwa. Z tego względu, przy stosowaniu urządzeń ATM w sieciach lokalnych, szczególną uwagę należy poświęcić ich zarządzaniu [10].

Warto zaznaczyć, że moduły zarządzania nowoczesnych elementów sieciowych dają olbrzymie możliwości śledzenia zdarzeń zachodzących w sieci. Różne względy powodują, że mechanizmy te nie są w pełni i powszechnie wykorzystywane. Wynika to z konieczności lokalnego konfigurowania urządzeń ze względów bezpieczeństwa lub wskutek braku oprogramowania dla centralnego zarządzania siecią.

Często zdarza się, że przepracowany lub niedostatecznie wyszkolony administrator sieci nie podejmuje odpowiednich działań.

3.7. Świadomość użytkowników

Brak świadomości użytkowników ważności problemów zabezpieczeń sieci może powodować nieefektywność stosowanych mechanizmów. Zadaniem służb odpowiedzialnych za zabezpieczenie sieci musi być opracowanie i przeprowadzenie stosownego szkolenia pracowników. Celem tego szkolenia powinno być wyjaśnienie:

- celów, strategii i polityki zabezpieczeń stosowanych w przedsiębiorstwie;
- potrzeby zabezpieczenia oraz roli i odpowiedzialności poszczególnych pracowników.

3.8. Komputery osobiste w sieci lokalnej

Stosowanie **komputerów osobistych** w środowisku LAN niesie ze sobą dodatkowe ryzyko. Systemy operacyjne komputerów PC zwykle nie mają wbudowanych mechanizmów kontroli dostępu, uwierzytelniania użytkowników, prowadzenia rejestrów dostępu itp. W większości przypadków poziom zabezpieczenia w serwerze jest wyższy niż w komputerach PC. Użytkownicy PC powinni uzyskać ze strony administracji sieci LAN właściwe wskazówki i odpowiednie przeszkolenie w zakresie poziomu zabezpieczenia obowiązującego w środowisku LAN.

4. NARUSZENIA ZABEZPIECZEŃ W SIECIACH LOKALNYCH

4.1. Analiza zdarzeń

Analiza zdarzeń występujących w sieci LAN umożliwia ocenę skali i konsekwencji naruszeń jej zabezpieczeń. Zdarzenie może po-

wodować szkody krótkoterminowe, takie jak: ujawnienie, modyfikacja, zniszczenie danych, odmowa obsługi, i długoterminowe w postaci: utraty kontraktów, naruszenia prywatności, procesów sądowych, kar finansowych, zagrożenia ludzkiego życia itp. Aby właściwie ocenić stan zabezpieczenia sieci lokalnej, należy najpierw pogrupować możliwe zdarzenia, a następnie przeprowadzić analizę zagrożeń i słabości, które mogą spowodować naruszenia zabezpieczeń. Zdarzenia można pogrupować w następujące kategorie:

- **nieupoważniony dostęp do LAN** w wyniku braku właściwej identyfikacji użytkownika;
- **nieupoważniony dostęp do zasobów LAN** w wyniku niewłaściwej autoryzacji dostępu użytkownika, który jednak może być pełnoprawnym użytkownikiem sieci;
- **ujawnienie danych** w wyniku dostępu lub odczytania poufnych danych, przypadkowo lub rozmyślnie;
- **nieautoryzowana modyfikacja danych i oprogramowania** polegająca na zmianie, usunięciu lub zniszczeniu zasobów sieci, w tym danych i oprogramowania, dokonanych przez nieupoważnionego użytkownika sieci, przypadkowo lub rozmyślnie;
- **ujawnienie informacji przesyłanych za pośrednictwem LAN** w wyniku dostępu lub odczytu danych przesyłanych w sieci, dokonanych przez nieupoważnionego użytkownika, przypadkowo lub rozmyślnie.
- **oszustwa wykorzystujące transmisję w sieci LAN,** polegające na przesłaniu fałszywej informacji w imieniu prawdziwego, uprawnionego użytkownika sieci;
- **przerwanie funkcjonowania LAN** przez doprowadzenie do sytuacji, w której zasoby LAN nie są dostępne w czasie wymaganym zasadami funkcjonowania sieci.

- **Nieupoważniony dostęp do LAN**

Do uzyskania nieupoważnionego dostępu stosuje się powszechnie trzy metody: **odstąpienie hasła, odgadnięcie hasła i przechwycenie hasła.**

Metody postępowania doprowadzające do odstąpienia hasła przez umyślne wprowadzenie użytkownika sieci w błąd są określane nazwą *social engineering*. Uzyskanie hasła umożliwia nieupoważnionemu użytkownikowi dostęp do sieci LAN i korzystanie z przywilejów upoważnionego użytkownika.

Odgadnięcie hasła może zdarzyć się na skutek niewłaściwych zasad wyboru hasła, stosowania metod słownikowych lub kryptoanalizy.

Przychwytywanie hasła i identyfikatora rejestrującego użytkownika w czasie transmisji w postaci jawnego tekstu za pośrednictwem sieci jest następną metodą uzyskiwania nieupoważnionego dostępu. Także uzyskanie hasła transmitowanego w postaci zaszyfrowanej i podstawienie go jako hasła rejestrującego w innej sesji ("podszycie się" pod uprawnionego użytkownika) jest przechwyceniem hasła. Można zauważyć, że jest to chyba jedyny przypadek, w którym zdobycie informacji w postaci zaszyfrowanej daje możliwość nieupoważnionego dostępu do systemu.

Podsumowując, nieupoważniony dostęp do LAN może się zdarzyć się na skutek następujących słabości systemu:

- niewystarczającego mechanizmu identyfikacji i uwierzytelnienia lub jego braku;
- odstępowania haseł (np. na skutek stosowania metod *social engineering*);
- niewłaściwego zarządzania hasłami (hasła zbyt łatwe do odgadnięcia, brak okresu ważności haseł, brak bezpiecznych procedur unieważniania i zmiany haseł);

- istnienia pojedynczych komputerów PC, w których hasła nie są chronione w trakcie ładowania systemu operacyjnego *(boot time)*;
- niedostatecznego wykorzystania mechanizmów blokowania komputera PC na czas nieobecności użytkownika;
- dostępu użytkowników sieci do plików wsadowych komputerów PC;
- niedostatecznej kontroli urządzeń sieciowych (możliwość „wpięcia się" w linię lub na port koncentratora);
- niezabezpieczonych modemów (niedostatecznego nadzoru nad procesem wyrejestrowania się z systemu i rozłączenia linii);
- braku ograniczeń czasowych procesu rejestrowania się i zapisywania prób dostępu;
- braku procedur rozłączenia w przypadku wielokrotnych prób zarejestrowania się;
- braku zapisów „data/czas ostatniej rejestracji zakończonej sukcesem" oraz „próba dostępu zakończona niepowodzeniem" (takich mechanizmów brak np. w popularnym, sieciowym systemie operacyjnym Windows for Workgroups);
- braku mechanizmu weryfikacji użytkowników w czasie rzeczywistym (w celu uniknięcia „maskarady"*));

- **Nieupoważniony dostęp do zasobów LAN**

Jedną z korzyści, jaką daje sieć lokalna, jest dostępność zasobów wspólnych dla wielu użytkowników. Dostępność zasobów jest kontrolowana przez mechanizmy przywilejów. Nieupoważniony dostęp do zasobów może zdarzyć się na skutek następujących słabości systemu:

---

*) „Maskarada" - próba podszycia się pod innego użytkownika w celu uzyskania nieuprawnionego dostępu [11].

- użycia standardowych, z reguły bardzo prostych zezwoleń na dostęp, które nie są restrykcyjne dla użytkowników;
- niewłaściwego wykorzystania przywilejów administratora lub zarządcy LAN;
- niedostatecznego poziomu zabezpieczenia składowanych danych;
- niewłaściwie stosowanego mechanizmu przydzielania przywilejów użytkownikom lub jego braku;
- obecności w sieci komputerów PC, w których brak kontroli dostępu na poziomie plików (często nie ma nawet kontroli dostępu na poziomie katalogów).

- **Ujawnienie danych**

Niektóre dane składowane lub przetwarzane w sieci lokalnej wymagają poufności. Ujawnienie poufnych danych może zdarzyć się dzięki uzyskaniu dostępu do nieszyfrowanych informacji, przeglądaniu ekranów lub wydruków. Ujawnienie danych może zdarzyć się na skutek następujących słabości systemu:

- niewłaściwego ustawienia parametrów kontroli dostępu;
- składowania danych, które powinny być zaszyfrowane w postaci jawnej;
- składowania kodów źródłowych aplikacji w postaci niezaszyfrowanej;
- ulokowania monitorów w powszechnie dostępnych miejscach;
- ulokowania drukarek w powszechnie dostępnych miejscach;
- przechowywania kopii zapasowych danych i programów w dostępnych miejscach.

- **Nieautoryzowana modyfikacja danych i oprogramowania**

Wspólny dostęp wielu użytkowników do danych i aplikacji wymaga kontroli wykorzystania zasobów. Nieautoryzowana modyfikacja, nie wykryta przez długi czas, może prowadzić do naruszenia integral-

ności systemu, a więc do sytuacji, w której system nie gwarantuje poprawności przedstawianej informacji. **Utrata integralności jest jednym z najpoważniejszych przypadków naruszenia systemu zabezpieczenia sieci lokalnych.**

Nieautoryzowana modyfikacja danych i oprogramowania może zdarzyć się na skutek następujących słabości systemu:

- udzielenia przywileju zapisu tym użytkownikom, którzy wymagają jedynie zezwolenia na odczyt;
- braku możliwości wykrycia zmian w oprogramowaniu, w tym dopisania kodu w celu uzyskania programu "konia trojańskiego"*);
- braku skutecznych narzędzi wykrywania i przeciwdziałania wirusom.

Problem zagrożenia dla sieci lokalnej, jakim są **wirusy komputerowe** wymaga szerszego omówienia. Wirusy i ich szkodliwy wpływ na pracę systemów komputerowych jest znany od wielu lat. Jednakże, w ostatnim roku pojawiły się nowe ich rodzaje, które ze względu na swój zasięg i sposób "zarażania" zasobów stanowią ogromne zagrożenie dla sieci lokalnych.

Wirusy od lat rozpowszechniały się głównie za pośrednictwem zarażonych dyskietek. Najczęściej spotykane wirusy prowadziły do uszkodzeń sektorów ładowalnych (*boot*) dyskietek. Szybkość rozpowszechniania wirusów nie była duża. Wiele przedsiębiorstw prowadziło restrykcyjną politykę w zakresie wymiany dyskietek, przynoszenia do miejsc pracy obcych dyskietek, rozpowszechniania nielegalnego (bez licencji) oprogramowania, chroniąc się w ten sposób przed wirusami. Panowała powszechnie opinia, że wirusy są plagą systemów DOS-owych i nie dotyczą sieci UNIX-owych. W ostatnim roku sytuacja się zmieniła.

---

*) „Koń trojański" - program, sprawiający wrażenie, że wykonuje użyteczne funkcje (czasami nawet to naprawdę robi), ale ponadto zawierający ukryte funkcje, które realizują cele niezgodne z interesem użytkowników lub właściciela sieci.

Po pierwsze, do sieci lokalnych dostały się wirusy makro. Wirusy makro w olbrzymiej większości są związane z najpopularniejszym procesorem tekstu Microsoft Word, ale pojawiły się także wirusy Microsoft Excel i Lotus Notes. Wirusy makro dołączają się do dokumentów. A dokumenty można:

- ściągnąć w postaci plików z Internetu;
- otrzymać w poczcie elektronicznej;
- uzyskać od innych użytkowników sieci lokalnej w trybie pracy grupowej.

Jeden z czołowych autorytetów w dziedzinie badania i przeciwdziałania wirusom, Wesselin Bonczew [4], przedstawił kilkanaście sposobów zarażania dokumentów Winworda, nawet wersji Office 97 oraz wykazał nieskuteczność mechanizmów antywirusowych oferowanych przez producenta. W efekcie, wirusy makro należą od roku do "najpopularniejszych" wirusów. Należy zauważyć, że zarażone dokumenty rozpowszechniają się niezależnie od platformy systemu operacyjnego.

Tablica 3

Sposoby rozpowszechniania się wirusów komputerowych

Droga infekcji	Procent przypadków
Dyskietki	69
Ściąganie plików	10
Poczta elektroniczna	9
Nieznana	12

Po drugie, ostatnie badania [2] (tabl. 3) wykazały znaczącą zmianę źródeł zarażania wirusami. Obecnie duża ich część pochodzi z Internetu. Jest to, moim zdaniem, największe obecnie zagrożenie internetowe dla zasobów komputerowych (głównie sieci lokalnych). Dotyka

bowiem wszystkich użytkowników Internetu, także tych, którzy uzyskują komutowany dostęp do Internetu (dynamicznie przyporządkowywany adres IP) albo korzystają wyłącznie z poczty elektronicznej. Rzecz dotyczy nie tylko wirusów makro, ale także wirusów ściąganych z plikami oraz apletów Java i ActiveX. Nowe źródło pochodzenia wirusów, Internet, ma zupełnie inną charakterystykę niż dotychczasowe źródła. Należy pamietać, że:

- wirusy internetowe (i intranetowe) rozpowszechniają się z szybkością nieporównywalnie większą niż dotychczas;
- wirusy te "zarażają" nie tylko pliki wykonawcze, ale także dokumenty, które do tej pory były wolne od wirusów;
- wirusy te instalują się w krótkim czasie w wielu tysiącach komputerów (jeśli są dołączone np. do plików uaktualniających popularny program archiwizujący, oprogramowania służącego do przeglądania plików graficznych o "specjalnych" walorach, oprogramowania "zdejmującego" ograniczenia możliwości programów wersji demo);
- dostępne są w Internecie miejsca, skąd można uzyskać kody źródłowe wirusów makro, skompilowane zestawy wirusów, podręczniki pisania wirusów, itp.;
- ze względu na niezwykłą szybkość rozprzestrzeniania się wirusów, producenci pakietów antywirusowych nie nadążają ze skutecznymi narzędziami ich zwalczania.

W ten sposób, w ciągu ostatniego roku, wirusy oraz "złośliwe" aplety stały się największym zagrożeniem dla integralności systemów informatycznych.

- **Ujawnienie informacji przesyłanych za pośrednictwem LAN**

Informacje przesyłane za pośrednictwem LAN mogą być podsłuchiwane i przechwytywane z mediów transmisyjnych sieci (podłączenie się do kabla sieciowego, nasłuch radiowy w przypadku stosowa-

nia torów radiowych, dołączenie do sieci urządzeń analizujących itp.). Wielu użytkowników przywiązuje wagę do ochrony informacji składowanej na dyskach PC lub serwerów; jednakże często zapominają o konieczności ochrony przesyłanej informacji. Bywa tak, że hasła są przechowywane w zaszyfrowanej postaci, ale ze stacji roboczej do serwera przesyłane jako jawny tekst. Błąd ten powtarzał się w wielu starszych wersjach sieciowych aplikacji poczty elektronicznej. Ujawnienie informacji przesyłanych za pośrednictwem sieci LAN może zdarzyć się na skutek następujących słabości systemu:

- niedostatecznej fizycznej ochrony urządzeń i mediów transmisyjnych sieci LAN;
- użycia protokołów, w których dane są rozsyłane w postaci jawnego tekstu;
- transmisji w sieci LAN niezaszyfrowanych danych.

- **Oszustwa wykorzystujące transmisję w sieci LAN**

Dane przesyłane za pośrednictwem sieci LAN nie powinny ulec zniekształceniu, zarówno w wyniku samej transmisji, jak i działania nieupoważnionego intruza. Użytkownicy sieci LAN muszą dysponować metodami, umożliwiającymi potwierdzenie, że przesłana wiadomość nie została zniekształcona.

Oszustwa wykorzystujące transmisję w sieci LAN obejmują: **zdolność do odebrania wiadomości przez udawanie uprawnionego odbiorcy, udawanie uprawnionego nadawcy i wysyłanie w jego imieniu własnych wiadomości.**

Aby udawanie odbiorcy powiodło się, system zarządzania siecią musi przyjąć adres intruza jako prawdziwy adres odbiorcy. Odbieranie wiadomości może być też realizowane przez podsłuch informacji rozsyłanej do wszystkich węzłów sieci. Udawanie nadawcy wymaga wprowadzenia w błąd odbiorcy co do tożsamości drugiej strony lub zastosowania playbacku. Obie metody zostaną pokrótce omówione.

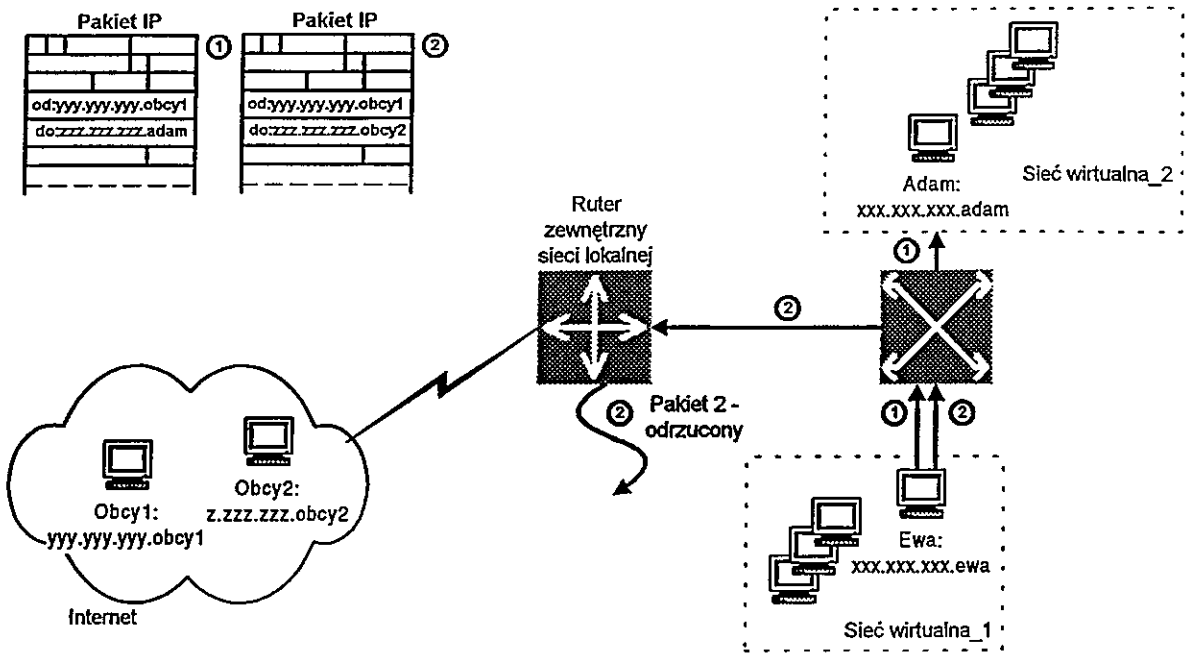
Udawanie nadawcy można zrealizować przez podstawianie fałszywych adresów eternetowych - często interfejsy urządzeń umożliwiają programowanie adresów MAC. A nawet jeśli jest to niemożliwe, to można zawsze zastąpić zainstalowany na płycie układ scalony odpowiednim programowanym układem.

Ze względu na zastosowanie w sieci lokalnej protokołu TCP/IP, są prawdopodobne różnego rodzaju oszustwa adresów IP znane z Internetu (*IP forging*). Zmiana adresu źródłowego IP jest operacją prostą nawet dla niedoświadczonych użytkowników sieci (publicznie są dostępne takie programy, jak np. iptest). Przykładowo, w sieci lokalnej, o konfiguracji takiej jak na rys. 3, mogłyby zdarzyć się ataki, których elementem składowym jest fałszerstwo adresów IP [21]. Na rys. 6 przedstawiono zakończoną powodzeniem próbę sfałszowania adresu IP w sieci lokalnej. Należy podkreślić, że definiowane na "zaporze ogniowej" (ruterze) reguły filtrowania ruchu z i do sieci WAN powodują odrzucenie pakietów o tak skonstruowanych, fałszywych adresach.

Z kolei, playback polega na zarejestrowaniu starej sesji nadawcy i odbiorcy oraz retransmisji wiadomości (całej lub z nowym nagłówkiem). Ataki powtórzeniowe są groźne dla protokołu TCP (np. słynny atak Kevina Mittnicka na centrum komputerowe w San Diego [21]). Ostatnio opisano zagrożenie tego typu dla nowego mechanizmu uwierzytelnienia IPsec [17].

Podsumowując, oszustwa wykorzystujące transmisję w sieci LAN mogą zdarzyć się na skutek następujących słabości systemu:

- transmisji wiadomości za pośrednictwem sieci LAN w postaci jawnego tekstu;
- braku znaczników czasowych (oznaczających czas nadania i odbioru wiadomości);
- braku mechanizmu kodu uwierzytelniania wiadomości *(MAC - Message Authentication Code)* lub podpisu cyfrowego;



Rys. 6. Przykład fałszerstwa adresu IP w sieci lokalnej

- braku mechanizmu weryfikacji w czasie rzeczywistym (w celu przeciwdziałania powtórzeniom).

- **Przerwanie funkcjonowania sieci LAN**

Przerwanie funkcjonowania sieci LAN może dotyczyć jednej lub wielu funkcji. Przerwanie funkcjonowania sieci LAN może zdarzyć się na skutek słabości systemu zarządzania siecią:
- braku możliwości wykrycia niezwykłego natężenia ruchu (np. zamierzonego zalewu informacją); ataki z grupy określanej nazwą "odmowa usługi" *(denial of service)* to np. atak SYN na protokół TCP/IP;
- braku możliwości przekierowania ruchu, procedur wyłączenia z eksploatacji uszkodzonych urządzeń, itp.;
- nieodporności konfiguracji sieci LAN na pojedyncze uszkodzenia sieci;
- dokonywania zmian sprzętowych przez nieuprawnione osoby (zmiany adresów stacji roboczych, modyfikacja ustawień ruterów i koncentratorów itp.);
- niewłaściwego utrzymania zasobów sprzętowych sieci LAN;
- niewłaściwego fizycznego zabezpieczenia sprzętu sieciowego LAN.

5. MECHANIZMY I USŁUGI SYSTEMU ZABEZPIECZEŃ

Usługi systemu zabezpieczeń, na które składają się mechanizmy, procedury i związane z nimi bazy danych zmniejszają ryzyko związane z zagrożeniami oraz słabościami sieci LAN. Podstawowymi usługamii systemu zabezpieczeń sieci LAN są [11]:
- **identyfikacja i uwierzytelnianie,** tj. usługa systemu zabezpieczeń, zapewniająca dostęp do sieci tylko uprawnionym użytkownikom;

- **kontrola dostępu**, tj. usługa systemu zabezpieczeń, zapewniająca autoryzowany dostęp do zasobów sieci;
- **poufność danych i wiadomości**, tj. usługa systemu zabezpieczeń, zapewniająca, że dane, oprogramowanie i przesyłane wiadomości nie zostaną ujawnione nieupoważnionym użytkownikom;
- **integralność danych i wiadomości**, tj. usługa systemu zabezpieczeń, zapewniająca, że dane, oprogramowanie i przesyłane wiadomości nie zostaną zmodyfikowane przez nieupoważnionych użytkowników;
- **niezaprzeczalność**, tj. usługa systemu zabezpieczeń, w której komunikujące się strony nie mogą zaprzeczyć: nadawca, że wysłał wiadomość (niezaprzeczalność z dowodem wysłania), odbiorca, że ją otrzymał (niezaprzeczalność z dowodem odbioru);
- **rejestrowanie i monitorowanie**, tj. usługa systemu zabezpieczeń, umożliwiająca śledzenie wykorzystania zasobów w całej sieci;
- **zarządzanie kluczami**, tj. usługa administrowania i użytkowania kluczy kryptograficznych. Na usługę tę składa się 11 usług związanych z kluczami: generowanie, rejestrowanie, certyfikowanie, wyrejestrowywanie, rozpowszechnianie, instalowanie, przechowywanie, archiwizowanie, tworzenie kluczy pochodnych z klucza nadrzędnego i niszczenie.

5.1. Identyfikacja i uwierzytelnianie

Pierwszym krokiem w kierunku zabezpieczenia zasobów sieci LAN jest uzyskanie zdolności weryfikacji tożsamości, czyli uwierzytelnienie. W sieci lokalnej uwierzytelnienie jest pojmowane dość wąsko i oznacza przeważnie uwierzytelnienie użytkownika wobec serwera lub, rzadziej, uwierzytelnianie wzajemne użytkownika i serwera. W standardach uwierzytelnianie jest pojmowane znacznie szerzej, jako uwierzytelnianie podmiotów i danych. Należy podkreślić, że uwierzytelnienie stanowi podstawę efektywności innych procedur

kontrolnych w sieci LAN. Przykładowo, mechanizm rejestrowania opiera się na identyfikatorze użytkownika *(userid)*. Analogicznie jest w przypadku mechanizmu kontroli dostępu do zasobów LAN. Oba te mechanizmy będą efektywne pod warunkiem, że żądający usługi jest uprawnionym użytkownikiem sieci LAN z przyporządkowanym jednoznacznie identyfikatorem.

Identyfikacja żąda od użytkownika jednoznacznej nazwy stosowanej w każdym przypadku korzystania z zasobów sieci. Jednakże, system nie może przyjąć identyfikatora użytkownika tylko na podstawie jego twierdzenia, bez uwierzytelnienia. Powszechnie znana jest charakterystyka uwierzytelnienia jako dowodu tożsamości: użytkownik potrafi wylegitymować się czymś, co tylko on ma, (np. tokenem*)), czymś, o czym tylko on wie, (np. hasłem) lub czymś, co jednoznacznie go identyfikuje, (np. odcisk palca).

Biorąc pod uwagę specyfikę środowiska sieciowego, można zaproponować nieco inną klasyfikację, opierając się na różnicy w przesyłanej informacji:

- **mechanizmy oparte na parametrach biometrycznych;**
- **mechanizmy oparte na wiedzy:**
  - hasła, PIN;
  - hasła jednorazowe;
- **mechanizmy oparte na dowodzie wiedzy:**
  - z tajnym kluczem;
  - z publicznym kluczem, wykorzystujące: certyfikat, tożsamość, wiedzę zerową.

W niektórych systemach uwierzytelnienie opiera się na parametrach biometrycznych użytkowników. Systemy takie są kosztowne, niestandardowe i raczej nie stosowane jeszcze w sieciach LAN.

---

*) Token (przekaz) - pole danych przesyłane w trakcie procedury uwierzytelnienia, zawierające informację, która jest przekształcana z wykorzystaniem technik kryptograficznych.

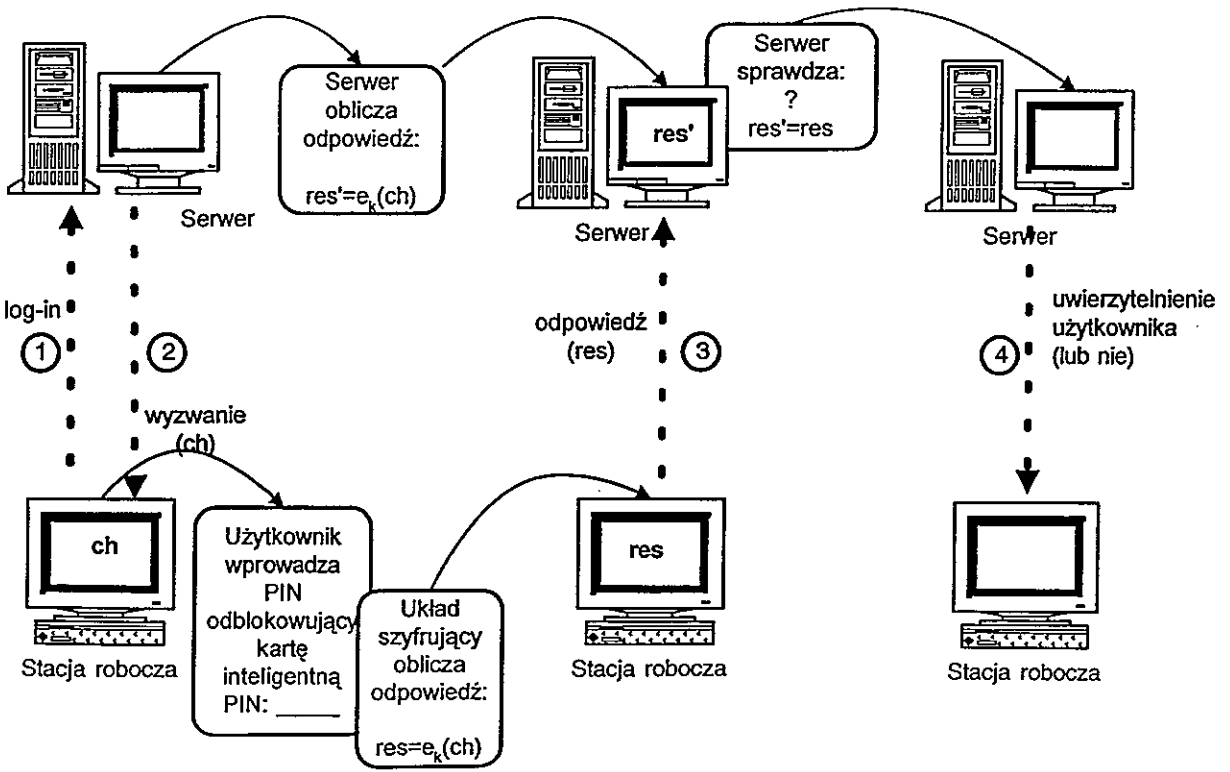
Mechanizm identyfikacji i uwierzytelnienia zwykle stosowany w sieciach LAN jest oparty na wiedzy. Przykładem takiego mechanizmu jest schemat identyntyfikatora/hasła. Mechanizm uwierzytelnienia, który opiera się jedynie na hasłach często nie daje wystarczającego zabezpieczenia. Użytkownicy mają skłonność do tworzenia haseł, które łatwo zapamiętać, ale też i łatwo odgadnąć. Hasła trudne do odgadnięcia są też trudne do zapamiętania. Właściwy wybór hasła to kompromis między dwiema skrajnościami. Stosowane są generatory haseł, które tworzą hasła na podstawie pseudolosowego wyboru znaków. Programy sprawdzające hasła umożliwiają wskazanie haseł łatwych do odgadnięcia, a zatem nieakceptowalnych.

Mechanizmy oparte tylko na hasłach, które w dodatku dopuszczają przesyłanie haseł w jawnej postaci, są szczególnie narażone na podsłuch i przechwytywanie. Jest to poważny problem dla sieci LAN, także tych, które mają połączenie ze światem zewnętrznym. W takim przypadku właściwe zarządzanie procesami tworzenia, składowania, nadawania terminu ważności i unieważniania haseł jest krytycznym elementem systemu zabezpieczeń.

Niedostatki powtarzalnych haseł eliminuje metoda haseł jednorazowych. Ponieważ hasło jest tu użyte tylko raz, zawodzą metody przechwytywania. Należy zaznaczyć, że w dalszym ciągu istnieje zagrożenie przechwycenia sesji, gdyż procedura uwierzytelnienia jest realizowana jedynie na początku sesji łączności [21].

W mechanizmach uwierzytelniania opartych na dowodzie wiedzy uwierzytelnieniu nie podlega użytkownik, ale inteligentne urządzenie, którego używa. W przypadku uwierzytelniania przy użyciu tajnego klucza, klucz jest wykorzystywany jako argument funkcji transformującej. Innym argumentem tej funkcji może być parametr zmienny w czasie (znacznik czasowy lub liczba pseudolosowa).

W mechanizmach opartych na dowodzie wiedzy stosuje się metodę „wyzwanie - odpowiedź". Komunikujące się strony wykorzystują do uwierzytalniena posiadane tokeny (tokenem może to być np. zapis



Rys. 7. Uwierzytelnienie jednostronne użytkownika w postaci dowodu wiedzy z wykorzystaniem schematu „wyzwanie - odpowiedź"

na karcie magnetycznej lub elektronicznej). Na rys. 7 przedstawiono procedurę uwierzytelniania zwaną SN-Key [6]. Procedura rozpoczyna się wprowadzeniem przez użytkownika identyfikatora, a następnie odblokowaniem karty elektronicznej za pomocą kodu PIN. System wysyła wyzwanie, które jest wpisywane na tę kartę. Wyzwanie jest szyfrowane przy użyciu algorytmu DES kluczem przechowywanym na karcie i odsyłane do serwera. Jeśli otrzymana odpowiedź jest identyczna z wynikiem obliczeń przeprowadzonych przez serwer, użytkownik jest uwierzytelniony. Dodanie znaczników czasowych do procedur opartych na metodzie "wyzwanie - odpowiedź" uniemożliwia atak powtórzeniowy.

Mechanizmy dowodu tożsamości wykorzystujące kryptografię publicznego klucza: tworzenie certyfikatów*) [12] użytkownika wymaga udziału zaufanej strony trzeciej.

Procedura uwierzytelniania z dowodem wiedzy zerowej przebiega zgodnie ze schematem "wyzwanie - odpowiedź". Procedura ta gwarantuje, że podmiot weryfikujący nie uzyskuje żadnej dodatkowej wiedzy. Dowody wiedzy zerowej w protokole weryfikacji tożsamości zostały opisane w pracy [18].

Poza mechanizmami uwierzytelniania należy wprowadzić do sieci lokalnej uzupełniające procedury organizacyjne oraz mechanizmy wspomagające, a mianowicie:

- blokowanie urządzeń sieciowych;
- blokowanie komputera PC lub stacji roboczej;
- przerwanie połączenia po wielokrotnych próbach zarejestrowania się zakończonych niepowodzeniem;

---

*) Certyfikat - klucz publiczny oraz inne informacje identyfikujące użytkownika, zaszyfrowane kluczem prywatnym urzędu certyfikującego. Szyfrowanie uniemożliwia sfałszowanie certyfikatu [12].

- informowanie użytkownika o ostatniej, zakończonej sukcesem, rejestracji i liczbie prób zarejestrowania się zakończonych niepowodzeniem.

Wiele urządzeń sieciowych ma możliwość zablokowania nieużywanych portów i alarmowania systemu zarządzania siecią w przypadku wykrycia dołączenia się do takiego portu. Ponadto, okablowanie strukturalne umożliwia gromadzenie aktywnych elementów sieciowych w jednym miejscu i fizyczną ich ochronę.

Blokowanie może dotyczyć stacji roboczych lub komputerów PC. Blokując klawiaturę swego komputera i opuszczając miejsce pracy, użytkownik może pozostać zarejestrowany w systemie i mieć pewność, że żadna nieuprawniona osoba nie skorzysta z jego nieobecności.

Mechanizmy, które informują użytkownika o stanie jego sieciowego konta umożliwiają wykrycie nienormalnych zdarzeń (np. wielokrotne próby dostępu zakończone niepowodzeniem). Stan konta obejmuje: zapis daty, godziny i miejsca ostatniej, zakończonej sukcesem rejestracji oraz liczbę poprzednich prób zakończonych niepowodzeniem.

5.2. Kontrola dostępu

Usługa kontroli dostępu chroni przed nieupoważnionym dostępem do zasobów sieci LAN. Jest ona realizowana na podstawie mechanizmów kontroli dostępu i przydzielania przywilejów. W sieciach lokalnych stosuje się następujące mechanizmy:

- listę kontroli dostępu,
- schemat posiadanych uprawnień,
- mechanizm oparty na etykietach,
- kontrolę dostępu opartą na informacji kontekstowej.

Listy kontroli dostępu przyporządkowują prawa dostępu użytkownikom i grupom użytkowników identyfikowanych przez nazwy. Mechanizm kontroli dostępu w postaci list można stosować w sytuacji, gdy:

- jest pożądana kontrola dostępu o dużej szczegółowości,
- liczba użytkowników i grup żądających dostępu jest niewielka,
- jest pożądana łatwość unieważniania dostępu do zasobów,
- dostęp definiuje się, biorąc pod uwagę raczej ewidencję zasobów niż listę użytkowników.

Powyższego schematu nie należy stosować, gdy grupy użytkowników podlegają dynamicznym zmianom.

Schemat posiadanych uprawnień definiuje zbiór operacji dozwolonych danemu użytkownikowi (lub grupie użytkowników) na wskazanych zasobach (obiektach). Mechanizm ten warto stosować, gdy:

- liczba wskazanych zasobów (obiektów) jest niewielka,
- zarządzanie kontrolą dostępu koncentruje się na użytkownikach,
- duża liczba użytkowników lub grup użytkowników żąda dostępu do relatywnie małej liczby zasobów (obiektów) i użytkownicy ci znajdują się w różnych domenach systemu bezpieczeństwa,
- zachodzi konieczność częstego odwoływania prawa dostępu użytkowników do zasobów.

Z kolei mechanizm ten nie jest przydatny w sytuacji, gdy należy odwołać dostęp do wskazanego obiektu.

Mechanizm oparty na etykietach wykorzystuje etykiety "wrażliwości" (bezpieczeństwa) przyporządkowane użytkownikom, zasobom (obiektom) i przenoszonym danym. Kontrola dostępu polega na porównywaniu etykiet. Jest stosowana w systemach z obligatoryjną kontrolą dostępu. Schemat ten jest szczególnie przydatny, gdy:

- w systemie jest wielu użytkowników z możliwością dostępu do wielu zasobów, bez potrzeby dokładnego określania ziarnistości dostępu;
- w systemie jest konieczna kontrola przepływu danych między domenami bezpieczeństwa;
- dozwolone operacje nie określają dokładnie użytkownika i zasobu, ale są częścią zdefiniowanej polityki bezpieczeństwa.

Kontrola dostępu oparta na informacji kontekstowej polega na udzieleniu zezwolenia na podstawie informacji kontekstowej. Przykładami informacji kontekstowej mogą być:

- **przedział czasowy**: zezwolenie na dostęp jest udzielane tylko w ściśle określonym przedziale czasowym;
- **trasa**: zezwolenie na dostęp jest udzielane tylko wtedy, gdy użyta trasa ma ściśle określoną charakterystykę;
- **miejsce**: zezwolenie na dostęp mają tylko użytkownicy określonych systemów, stacji roboczych lub terminali;
- **stan systemu**: zezwolenie na dostęp jest udzielane tylko w wyjątkowych przypadkach (np. w trakcie procedury wyjścia z sytuacji awaryjnej);
- **zezwolenie na dostęp**: zezwolenie na dostęp jest udzielane pod warunkiem udzielenia zezwolenia innym użytkownikom.

Mechanizmy kontroli dostępu przeważnie należy implementować łącznie z innymi mechanizmmi, np. uwierzytelnienia lub integralności (szczególnie w przypadku schematu opartego na etykietach).

5.3. Poufność danych i wiadomości

Usługa poufności danych i wiadomości jest wprowadzana wszędzie tam, gdzie potrzebne jest utajnianie informacji. Usługa ta jest wspomagana przez mechanizmy kontroli dostępu, ale zasadnicze zabezpieczenie jest oparte na mechanizmach stosujących różnorodne algorytmy szyfrowania. W pierwszym rzędzie umożliwiają one szyfrowanie składowanych danych. Stosowanie algorytmów szyfrowania do realizacji usługi poufności jest niezbędne w przypadku tych komputerów PC, w których nie ma usługi kontroli dostępu.

Użycie mechanizmów szyfrowania zmniejsza ryzyko związane z niemożnością kontrolowania nieuprawnionego dostępu do informacji przesyłanej za pośrednictwem sieci LAN. Odczyt zaszyfrowanych

wiadomości transmitowanych w sieci jest możliwy tylko w przypadku złamania algorytmu szyfrowania. Uprawniony odbiorca ma klucz, który umożliwia odszyfrowanie, a następnie odczytanie wiadomości.

Algorytmy szyfrowania dzielą się na symetryczne (operacja szyfrowania i odszyfrowania jest realizowana za pomocą tego samego klucza szyfrowania) oraz asymetryczne (do operacji szyfrowania jest używany klucz, zwany publicznym, a odszyfrowanie następuje po zastosowaniu innego klucza, zwanego prywatnym). Jeśli zachodzi potrzeba szyfrowania danych należących do kategorii wrażliwych, ale nie poufnych, zaleca się [7] stosowanie algorytmu szyfrującego DES.

Algorytm szyfrowania asymetrycznego opiera się na wykorzystaniu pary związanych ze sobą kluczy: publicznego i prywatnego. Pierwszy z nich jest znany wszystkim, drugi, tajny, znany tylko swemu właścicielowi. Nie istnieje algorytm obliczeniowy, dzięki któremu przy znajomości klucza publicznego można uzyskać klucz prywatny w czasie gwarantującym jeszcze jego użyteczność. Każdy użytkownik ma własną parę kluczy. Jednakże, do tej pory organizacje standaryzujące nie zatwierdziły stosowania algorytmu asymetrycznego szyfrowania w mechanizmach gwarantujących poufność. Jest on wykorzystywany do tworzenia podpisów cyfrowych oraz mechanizmów gwarantujących niezaprzeczalność.

W zakresie polityki zabezpieczeń leży zdefiniowanie, w jakich procedurach archiwizacji należy stosować szyfrowanie danych przechowywanych na taśmach, dyskietkach, płytach CD-ROM itp. Poza szyfrowaniem należy stosować inne mechanizmy zapewniające poufność w sieci lokalnej. Dotyczy to zabezpieczenia przed ulotem informacji w wyniku emisji elektromagnetycznej oraz fizycznej ochrony urządzeń aktywnych sieci. Zabezpieczenia przed emisją ujawniającą obejmują: ekranowanie kabli, monitorów oraz zainstalowanie, w niektórych newralgicznych punktach sieci, generatorów szumowych.

Możliwe jest także wykorzystanie do celów poufności odpowiedniej konfiguracji elementów aktywnych sieci (nie tylko ruterów). Odpowiadając na zapotrzebowanie w zakresie zabezpieczenia sieci lokalnej, producenci dodają nowe funkcje do koncentratorów, mostów, przełączników i ruterów. Przykładowo, w bezpiecznych koncentratorach można ręcznie skonfigurować adresy MAC w portach. Adres przeznaczenia przychodzącego pakietu jest porównywany z listą adresów przyporządkowanych portom. Pakiet jest przepuszczany tylko przez port, który odpowiada adresowi docelowemu pakietu; reszta portów przekazuje nieznaczącą informację. Istnieją stosowne rozwiązania sprzętowe i programowe [9].

W sieciach ruterowych struktura adresowa sieci jest zbudowana w taki sposób, że wspólne obszary sieci mają wspólne adresowanie. Komunikacja miedzy segmentami o różnych adresach jest możliwa tylko za pośrednictwem rutera, który dokonuje translacji adresu warstwy trzeciej na adres MAC warstwy drugiej. W ruterach można definiować listy dostępu i zasady filtrowania oraz budować wewnętrzne "zapory ogniowe" sieci lokalnej. Powszechnie znane wady ruterów to ich wysoki koszt, wolne działanie oraz uciążliwe procedury zarządzania. Głównie z tej przyczyny zostały one wyparte na obrzeże sieci lokalnych (styk ze światem zewnętrznym) przez przełączniki - szybsze, tańsze, wprowadzające mniejsze opóźnienie. Sieć zbudowana na koncentratorach i przełącznikach opiera się w rzeczywistości na własnościach warstwy drugiej, co ewidentnie zwiększa ryzyko podsłuchu (por. pkt 3.5 i 4.1.5).

Aby rozwiązać ten problem, producenci przełączników wyposażyli je w możliwość definiowania sieci wirtualnych (rys. 3 i 4). Sieci wirtualne mają programową adresację warstwy trzeciej, która nie odpowiada fizycznej adresacji dołączonych urządzeń. Bezpieczeństwo warstwy trzeciej w sieciach wirtualnych jest realizowane programowo, zatem jest bardziej elastyczne. W typowych rozwiązaniach sieci wirtualnych LAN istnieje centralny punkt zarządzania, z którego

można konfigurować sieć wirtualną (przyporządkować adres MAC lub numer portu). Jest to więc, z punktu widzenia bezpieczeństwa, newralgiczne miejsce sieci. Ostatnio pojawiły się na rynku przełączniki realizujące sprzętowo funkcje warstwy trzeciej.

5.4. Integralność danych i wiadomości

Usługa integralności danych i wiadomości umożliwia ochronę danych i oprogramowania znajdujących się w stacjach roboczych, serwerach i innych elementach sieciowych przed nieupoważnioną modyfikacją, rozmyślną lub przypadkową. Usługa pozwala wykryć zmianę, usunięcie lub dodanie wiadomości w trakcie jej transmisji. Większość stosowanych obecnie mechanizmów zabezpieczeń wykrywa modyfikację wiadomości, ale nie potrafi skutecznie przeciwdziałać takim próbom.

Jednym z podstawowych mechanizmów kontroli integralności jest funkcja skrótu (*hash function*)*). Występują dwa podstawowe typy jednokierunkowych funkcji skrótu [13]: bez klucza i z kluczem. W pierwszym przypadku wartość skrótu jest funkcją ciągu wejściowego. W drugim przypadku funkcja ma dwa argumenty: ciąg wejściowy i klucz. Funkcja skrótu musi być dobierana w bardzo staranny sposób. Jest to funkcja pseudolosowa - prawdopodobieństwo wartości skrótu ma rozkład równomierny. Przykładem bezkluczowej funkcji skrótu jest zwykła suma kontrolna. Nie jest to jednak dobra funkcja skrótu z punktu widzenia mechanizmu integralności danych.

W mechanizmach detekcji modyfikacji stosuje się też kryptograficzną sumę kontrolną. Kod uwierzytelnienia wiadomości (*MAC - Massage Authentication Code*), jeden z typów sumy kontrolnej, za-

*) Funkcja skrótu - matematyczne przekształcenie, które odwzorowuje duży zbiór wartości w zbiór mniejszy.

pewnia ochronę przed nieupoważnioną modyfikacją danych. Zastosowanie algorytmu szyfrowania tajnym kluczem użytkownika umożliwia obliczenie początkowej wartości MAC. Wartość ta jest dołączana do wiadomości. Weryfikacja danych polega na obliczeniu wartości MAC dla odebranej wiadomości i porównaniu jej z wartością początkową. Jeśli obie liczby są identyczne, wiadomość zostaje uznana za autentyczną. Nierówność obu kodów MAC oznacza nieupoważnioną modyfikację wiadomości. Jest niemożliwe uzyskanie początkowej wartości MAC dla zmienionej wiadomości, bez znajomości tajnego klucza.

Modyfikację danych lub wiadomości można wykryć także za pomocą mechanizmu podpisów cyfrowych. Podpis cyfrowy można generować za pomocą algorytmów szyfrowania asymetrycznego, jak i symetrycznego. W przypadku algorytmu asymetrycznego, do tworzenia podpisu cyfrowego dla danej wiadomości wykorzystuje się jeden z pary kluczy, klucz prywatny nadawcy. Tak utworzony podpis cyfrowy jest wysyłany wraz z wiadomością. Podpis może być zweryfikowany przez przekształcenie wykonane za pomocą klucza publicznego nadawcy. Jeśli podpis cyfrowy został zweryfikowany, to odbiorca uzyskuje potwierdzenie, że wiadomość została podpisana przez autentycznego nadawcę i w trakcie przesyłania nie została zmieniona. Mechanizm podpisu cyfrowego jest wykorzystywany przy implementacji dwóch usług: niezaprzeczalności i integralności wiadomości.

Ponadto, integralność danych i wiadomości zapewniają inne mechanizmy związane z kontrolą dostępu:

- szczegółowy mechanizm przywilejów,
- odpowiednie ustawienie parametrów kontroli dostępu (np. nieudzielanie nieuzasadnionych zezwoleń na zapis),

a także:

- oprogramowanie wykrywające wirusy komputerowe,
- stacje robocze bez instalowanych lokalnie dysków,
- stacje robocze bez napędów dyskowych.

5.5. Niezaprzeczalność

Usługa niezaprzeczalności polega na niemożliwości zaprzeczenia swego udziału w wymianie wiadomości, jeśli tak w rzeczywistości było. Usług ta nabiera szczególnego znaczenia w przypadku, gdy główną aplikacją sieciową jest poczta elektroniczna. Jest ona implementowana na podstawie mechanizmu podpisu cyfrowego opisanego w pkt. 5.4, opartego na algorytmie szyfrowania asymetrycznego. Usługa niezaprzeczalności może być implementowana w postaci zaufanej strony trzeciej.

5.6. Rejestrowanie i monitorowanie

Usługa rejestrowania i monitorowania pełni dwie funkcje. Pierwsza z nich to wykrywanie zdarzeń. W zależności od zakresu rejestrowania, wykryte zdarzenie może być śledzone w całym systemie. Przykładowo, jeśli dostęp do systemu uzyskała nieuprawniona osoba, to rejestr powinien sygnalizować, kto to jest, wskazywać listę wrażliwych plików, do których próba dostępu zakończyła się niepowodzeniem, wszystkie programy, które próbowano uruchomić, wszystkie programy, których uruchomienie zakończyło się sukcesem itp.

Drugą funkcją tej usługi jest dostarczanie zarządcy sieci danych do analizy statystycznej. Służy temu mechanizm audytu, traktujący plik rejestrowy jako informację wejściową i przetwarzający ją w zbiór parametrów charakteryzujący wykorzystanie sieci oraz stan jej zabezpieczenia. Funkcja monitorowania umożliwia wczesne wykrywanie problemów związanych z zabezpieczeniem zasobów sieci.

Zalety dobrego zarządzania siecią trudno przecenić. Najbardziej wymyślne procedury zabezpieczenia zawiodą, jeśli przykładowo, sieć można wyłączyć, nawiązując sesję telnet i odgadując proste hasło administratora. Sieć zarządzania musi być co najmniej tak dobrze zabezpieczona, jak sieć, która jest zarządzana.

Standardem *de facto* zarządzania dla sieci lokalnych jest SNMP (*Simple Network Management Protocol*) [20]. Nowa wersja tego protokołu SNMPv2 obejmuje też aspekty zabezpieczania sieci zarządzania. Opiera się na silnych mechanizmach uwierzytelniania i poufności. Centralne zarządzanie siecią lokalną opartą na systemie zarządzania SNMPv2 jest rozwiązaniem całkowicie nowym, bardzo kosztownym i jeszcze nie znajdującym powszechnego zastosowania.

5.7. Zarządzanie kluczami

Podstawową funkcją usługi zarządzania kluczami jest dostarczenie podmiotom **wspólnego tajnego klucza sesyjnego**. Kryptografia z wykorzystaniem technik symetrycznych pozwala zastosować dwie metody:

- bez centrum zarządzania kluczami: podmioty wykorzystują wspólny, tajny klucz, który jest im wcześniej znany;
- z centrum zarządzania kluczami: każdy z podmiotów dzieli wspólny, tajny klucz z centrum, ale nie między sobą; centrum działa jako zaufana strona trzecia, generując klucz albo przetwarzając klucz przesłany przez jeden z podmiotów.

Kryptografia z wykorzystaniem technik asymetrycznych pozwala zastosować procedury:

- uzgadniania klucza: podmioty uzgadniają klucz protokołem, bez konieczności wcześniejszego określenia jego wartości;
- przenoszenia klucza: tajny klucz sesyjny jest wybierany przez jeden z podmiotów i transmitowany do drugiego protokołem zabezpieczonym szyfrowaniem asymetrycznym.

Drugą podstawowową funkcją tej usługi jest rozpowszechnianie publicznych kluczy. Rozpowszechnianie to może być realizowane z udziałem zaufanej strony trzeciej lub bez takiego udziału. Brak dobrego zarządzania kluczami w sieciach lokalnych i rozległych jest głównym problemem rozwoju takich propozycji standardów, jak SSL

(*Secure Sockets Layer*), (wspólne przedsięwzięcie Netscape i Microsoft) czy SSH (*Secure Shell*) [17]. Szersze omówienie problemów związanych z zarządzaniem kluczami wykracza poza zakres niniejszego artykułu.

6. PODSUMOWANIE - POLITYKA ZABEZPIECZANIA SIECI LOKALNEJ

W artykule przybliżono problematykę zagrożeń, słabości i zabezpieczeń stosowanych w sieciach lokalnych. W praktyce, rozwiązanie problemu zabezpieczenia systemu informatycznego wymaga zdefiniowania **polityki zabezpieczenia**. Poza mechanizmami zabezpieczeń istnieje bowiem wiele czynników, wpływających w różnoraki sposób na stan bezpieczeństwa systemu informatycznego w przedsiębiorstwie.

Do takich czynników można zaliczyć:

1) uwarunkowania wewnętrzne:
   - cele i zadania przedsiębiorstwa; ogólne i w zakresie zabezpieczania swoich zasobów informatycznych;
   - kondycję finansową przedsiębiorstwa;
   - uzależnienie działania przedsiębiorstwa od systemu informatycznego;
   - stan świadomości kierownictwa w zakresie wagi zabezpieczenia systemu informatycznego;
   - możliwości techniczne i organizacyjne przedsiębiorstwa w zakresie planowania, wdrożenia i eksploatacji zabezpieczeń systemu informatycznego;
   - stan świadomości użytkowników systemu informatycznego;
2) uwarunkowania zewnętrzne:
   - stan legislacji;
   - politykę rządu;
3) właściwości systemu informatycznego:
   - infrastrukturę i topologię sieci;
   - system operacyjny sieci;

- system zarządzania siecią;
- charakterystyki stacji roboczych;
- stosowane aplikacje;

4) procedury, regulaminy:
   - korzystania z sieci;
   - postępowania w sytuacji naruszenia zabezpieczeń;
   - procedury wyjścia z sytuacji awaryjnej i katastrofalnej (zapewnienie ciągłości działania);
5) strukturę organizacyjną przedsiębiorstwa.

Słabość **polityki zabezpieczeń** może spowodować zwiększenie ryzyka poniesienia strat w przedsiębiorstwie z tytułu niewłaściwego funkcjonowania sieci LAN. Zadaniem kierownictwa jest sformułowanie jasnej polityki ochrony majątku przedsiębiorstwa, zakresu odpowiedzialności pracowników oraz dostosowanie organizacyjne przedsiębiorstwa do wymogów bezpieczeństwa.

Aby uwzględnić wpływ, jaki wyżej wymienione czynniki mogą mieć na stan zabezpieczenia systemu informatycznego, należy przeprowadzić analizę przedsiębiorstwa w zakresie funkcjonowania tego systemu. W przedsiębiorstwie powinny zostać zdefiniowane cele (co ma być osiągnięte), strategie (jak osiągnąć cele) i działania (co należy zrobić). Aby wprowadzić efektywne mierniki zabezpieczenia systemu informatycznego, należy dokonać scalenia różnych celów, strategii i działań definiowanych we wszystkich jednostkach organizacyjnych przedsiębiorstwa. Scalenie to powinno uzyskać formę jednolitego i uzgodnionego dokumentu określanego jako **Polityka Zabezpieczenia Systemu Informatycznego** [1]. Proces tworzenia takiego dokumentu, w którym polityka zabezpieczenia opiera się na zdefiniowaniu procesów zarządzania zabezpieczeniem systemu informatycznego, został w cytowanej pracy szczegółowo omówiony.

Dokument polityki zabezpieczenia systemu informatycznego, także sieci lokalnej, powinien zawierać część dotyczącą planowania zabez-

pieczenia. Proces planowania zabezpieczenia składa się z dwóch zasadniczych etapów: zarządzania (analizy) ryzykiem i planowania mechanizmów zabezpieczeń. W niniejszym artykule przedstawiono szczegółowy opis zjawisk zachodzących w sieci lokalnej i związanych z jej zabezpieczeniem. Na podstawie tego opisu można przystąpić do metodycznej analizy ryzyka i stworzyć plan zabezpieczenia sieci lokalnej, dostosowując sformalizowany model opisany w pracy [1] do specyfiki dowolnego przedsiębiorstwa.

Opracowanie planu zabezpieczenia sieci lokalnej Instytutu Łączności ma być jednym z efektów pracy statutowej nr 073017 pt. "Planowanie i zarządzanie zabezpieczeniami systemu informatycznego" rozpoczętej w 1997 roku.

WYKAZ LITERATURY

1. Andrukiewicz E.: Zarządzanie zabezpieczeniem systemu informatycznego. Prace IŁ, nr 108, 1997.
2. Aubrey-Jones D.: Internet - Virusnet? Network Security, February 1997.
3. Bellman R.: Making the Move to Switched Internetworking. Bay Networks Inc., 1995.
4. Bontchev V.: Protecting Networks from Virus Infection. The Second Annual Conference on Network Security, Cannes (Francja), 20-21 March 1997.
5. BS 7799 : 1995 Code of Practice for Information Security Management. BSI, 1995.
6. Cameron D.: Security Issues for the Internet and the World Wide Web. Computer Technology Research Corp., Charleston, South Carolina (USA), 1997.
7. Federal Information Processing Standard Publication 46-2: Data Encryption Standard (DES). 30 December 1993.
8. Federal Information Processing Standards Publication (FIPS PUB) 191: Specification for Guideline for The Analysis Local Area Network Security. November 1994.

9. Hansen L.: Network Infrastructure Security. The Second Annual Conference on Network Security, Cannes (Francja), 20-21 March 1997.
10. Hansen L.: The Impact of ATM Security in the Data Network. Network Security, January 1996.
11. ISO/IEC 7498-2 (ITU-T X.800): Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.
12. ISO/IEC 9594-8 (ITU-T X.509): Information technology - Open Systems Interconnection - The Directory: Authentication Framework.
13. ISO/IEC 10118: Information technology - Security techniques - Hash-functions.
14. ISO/IEC 10181-4 (ITU-T X.813): Information technology - Open Systems.
15. ISO/IEC TR 13335-1: Guidelines for the Management of IT Security, ISO/IEC Technical Report. 1996.
16. Minoli D., Alles A.: LAN, ATM and LAN Emulation Technologies. Artech House, Inc., Norwood (USA) 1996.
17. Reid J.: Plugging the Holes in Host-Based Authentication. Computers & Security, Vol. 15, No. 8, August 1996.
18. Schneier B.: Kryptografia dla praktyków. WNT, Warszawa 1995.
19. Shaffer S.L, Simon A.R.: Network Security. AP Professional, Londyn 1994.
20. Stallings W.: SNMP, SNMPv2 and RMON, Practical Network Management. Addison Wesley Publishing Company, Inc., Reading Massachusetts (USA), 1996.
21. Thomsen D.: IP Spoofing and Session Hijacking. Network Security, March 1995.