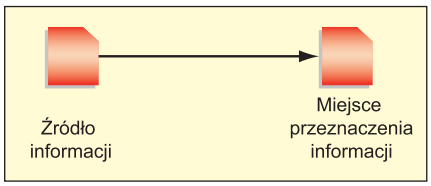
Bezpieczeństwo sieci komputerowej

Internet jako największa publiczna sieć komputerowa przyciąga coraz większe rzesze użytkowników, oferując im bogate zbiory informacyjne, grupy dyskusyjne, wymianę poczty elektronicznej, gry sieciowe czy też prowadzenie rozmów „on line". Zainteresowanie to powoduje wzrost ryzyka utraty prywatności lokalnych sieci komputerowych. Coraz częstsze ataki hakerów, rozpowszechniające się wirusy, spamy poczty elektronicznej stają się utrapieniem osób odpowiedzialnych za politykę bezpieczeństwa sieci.

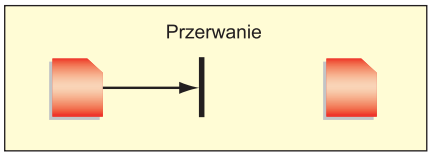
Zagrożenia z sieci

Zagrożenie płynące z sieci komputerowej połączonej z globalną siecią zwaną Internetem, są złożone i częstokroć niedoceniane. Regularnie odkrywane błędy w systemach w połączeniu ze sposobami omijania lub łamania zabezpieczeń pozwalają stwierdzić, że jednokrotna konfiguracja sieci nie zabezpieczy jej na zawsze. Jedynie tylko aktywna i systematyczna kontrola nad siecią jest w stanie zapewnić jej bezpieczeństwo.

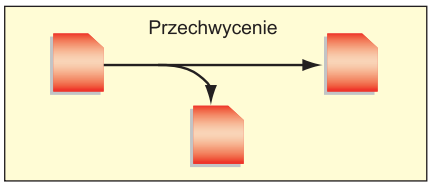
Klasyfikacja zagrożeń



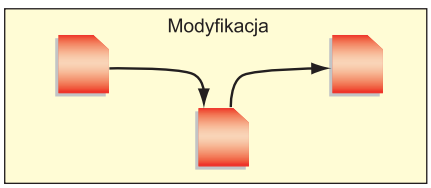
Rys. 1. Przepływ normalny, informacja w tym przypadku dociera do adresata (brak Ataku)



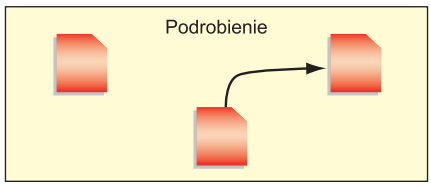
Rys. 2. Przepływ przerwany, informacja nie dociera do użytkownika (Atak na dyspozycyjność)



Rys. 3. Informacja dociera do odbiorcy, ale w tle zostaje przechwycona przez nieupoważnioną osobę (Atak na poufność)



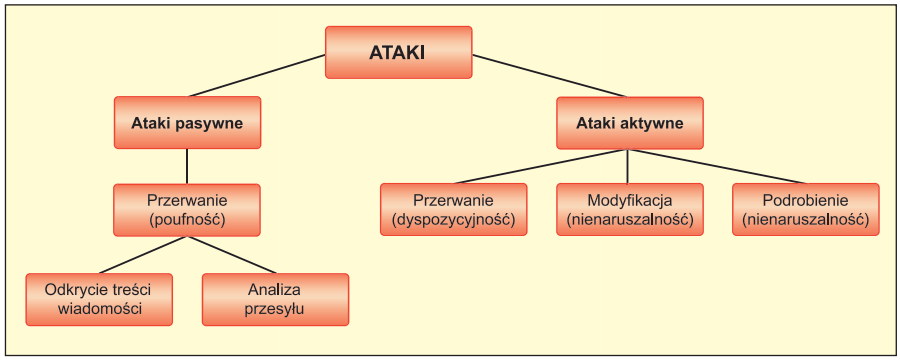
Rys. 4. Informacja docierająca do adresata zostaje zmodyfikowana bez jego wiedzy (Atak na nienaruszalność)



Rys. 5. Informacja docierająca do adresata jest podrobiona (Atak na autentyczność)

Klasyfikacja ataków

Budowa skutecznego systemu zabezpieczeń jest możliwa tylko wtedy, gdy wiemy, przed czym mamy się bronić i jakie rodzaje ataków nam zagrażają.



Rys. 6. Klasyfikacja ataków

Nasłuch

Jest bardzo często wykorzystywany do przechwytywania haseł. Dokonuje tego ukryty w systemie program (np. fałszywy program login), który odbiera wpisywane przez użytkownika dane udostępniając w ten sposób hasło.

Kolejną metodą jest prowadzenie nasłuchu sieci „nasłuchiwanie sieci – sniffing" w trakcie zdalnego połączenia legalnego użytkownika. Nasłuch sieci realizowany jest za pomocą urządzeń podsłuchowych, w trakcie trwania transmisji danych.

Urządzeniem takim może być odpowiednio zmodyfikowana karta sieciowa, umożliwiająca przechwytywanie pakietów.

Sniffing jest dużym zagrożeniem, ponieważ nie ogranicza się tylko do przechwytywania hasła. W przypadku prowadzenia nieszyfrowanej transmisji danych nasłuchiwanie sieci może doprowadzić do całkowitej utraty poufności przesyłanych informacji.

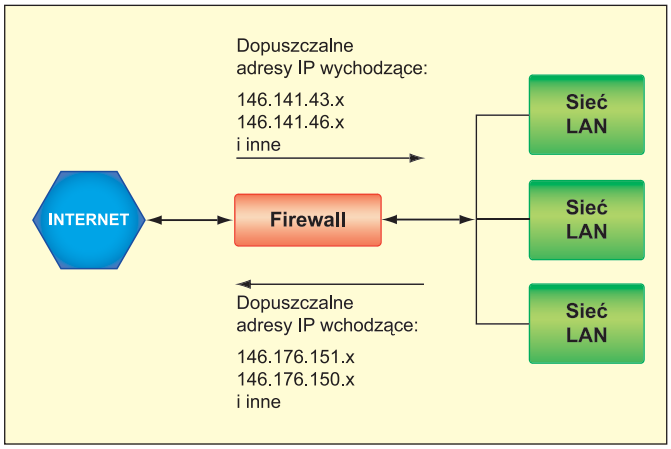
Nie ma niestety skutecznych narzędzi przeciwdziałania tej technice, a dostępne programy monitorujące prace sieci komputerowej nie gwarantują wykrycia dobrze zamaskowanego urządzania podsłuchowego.

Złośliwe programy

Wirus – jest to program dopisujący się do innego programu, który atakuje system w trakcie uruchamiania swojego żywiciela. W cyberprzestrzeni istnieje szeroka gama wirusów począwszy od wirusów mniej groźnych i łatwych do wykrycia, np. napisanych w Basicu i dołączonych jako makro do plików Worda, po bardziej skomplikowane, wyrządzające duże szkody w systemie operacyjnym. Jednocześnie są zdecydowanie trudniejsze do wykrycia, nawet przez najnowocześniejsze programy antywirusowe. Wirusy te są zazwyczaj napisane w językach niższego poziomu, np. C, Asembler. Odmianą tego typu szkodliwych programów są wirusy polimorficzne. Ich odmienność polega na tym, że nawet po podjęciu przez program antywirusowy procedury unicestwienia wirusa nie można całkowicie go usunąć, gdyż ciągle w sposób pseudo przypadkowy zmienia swój kod.

Bakteria – „królik" zasada działania tego programu polega na wielokrotnym kopiowaniu i uruchamianiu swojego własnego kodu źródłowego, celem pełnego zagarnięcia wszystkich zasobów komputera, takich jak: czas procesora, pamięć operacyjna, przestrzeń dyskowa, co w rezultacie doprowadza do spowolnienia lub zawieszenia systemu operacyjnego.

Koń trojański – program, który udaje pracę innego legalnego programu, a w międzyczasie wykonuje szereg niepożądanych czynności, np. kradnie hasło użytkownika. Zainfekowanie komputera wirusem może odbyć się poprzez pocztę elektroniczną, bądź podczas ściągania przez użytkownika sieci atrakcyjnego programu z niesprawdzonego źródła.



Rys. 7. Filtr pakietów

Bomba czasowa – programy tego typu charakteryzują się tym, że swoje destrukcyjne działanie uruchamiają tylko w ustalonym czasie, np. w dzień urodzin autora programu, bądź w przypadku spełnienia wcześniej założonych warunków.

Robak – program, który powiela samego siebie, wykonuje ustalone czynności określone przez twórcę programu (z reguły niekorzystne dla systemu) i próbuje przenieść się do innego komputera w sieci.

Furtki i włazy

Koleiną kategorią zagrożeń są tzw. „furtki", które umożliwiają kontrolowane wejście do legalnych programów. Są one tworzone przez programistów, np. w procesie testowania aplikacji. „Furtką" do programu może być ciąg znaków lub nawet wciśnięcie odpowiedniej kombinacji klawiszy. Odnalezienie takiej furtki daje nieuprawnionemu użytkownikowi kontrolę nad aplikacją.

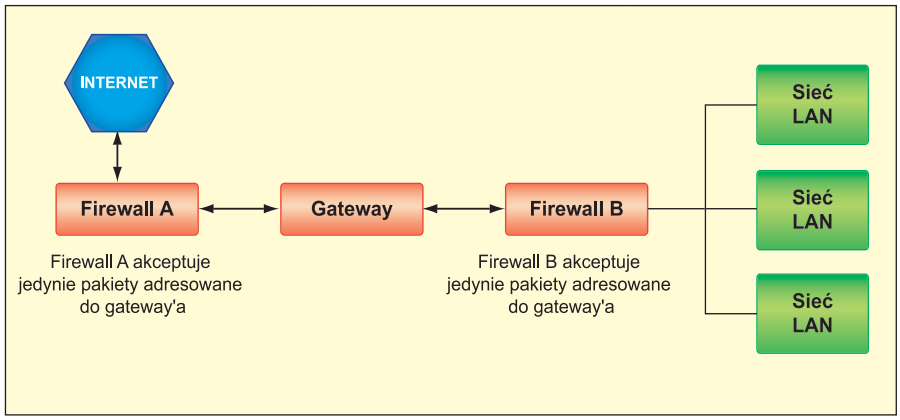
Spoofing

Jest to technika oszukiwania zabezpieczeń systemów, także tych chronionych przez „firewall". Określenie Spoofing wywodzi się z dziedziny wojskowej i oznacza „przeciwdziałanie elektronicznym przeciwsystemom nieprzyjaciela poprzez nadawanie fałszywych informacji". W odniesieniu do zagadnienia transmisji danych w sieci TCP/IP „IP Source-Address Spoofing", oznacza proces przesyłania pakietów zawierających nieprawdziwy adres źródłowy, przez co komputer odbierający te pakiety błędnie zidentyfikuje ich nadawcę.

Rodzaje zabezpieczeń

Bezpieczeństwo WWW

Serwery WWW udostępniają dane w formie dokumentów hipertekstowych. Dokument hipertekstowy jest zbiorem pojedynczych stron połączonych ze sobą odnośnikami (linkami). Strony zapisane są w języku HTML. Mogą zawierać różnego rodzaju informacje, takie jak tekst, dźwięk, elementy grafiki, aplikacje. Efektywność funkcjonowania WWW wynika z faktu, iż pojedyncze strony dokumentu hipertekstowego nie są przesyłane jako tradycyjne pliki graficzne, lecz w formie tekstu (opis) w języku HTML, na podstawie którego przeglądarka WWW odtwarza wygląd dokumentu. Każda strona dokumentu hipertekstowego jest jednoznacznie zidentyfikowana w całym obszarze sieci Internet na podstawie unikalnego adresu URL (Uniform Resource Location), np. http://www.wsisiz.edu.pl/index.html.



Rys. 8. Gateway poziomu aplikacji

Niestety HTTP i HTML nie zawierają żadnych wbudowanych mechanizmów pozwalających na utrzymywanie poufności, autentyczności czy też nienaruszalności przesyłanych danych. W rezultacie tak przesłane informacje mogą zostać swobodnie odczytane w trakcie transmisji i wykorzystane przez osoby nieupoważnione.

W tym przypadku odpowiednią ochronę możemy uzyskać stosując dodatkowe środki zabezpieczające. Obecnie najpopularniejszą propozycją jest technologia SSL (Secure Sockets Layer), umożliwiająca szyfrowanie i uwierzytelnianie przekazywanych informacji oraz ustalanie prawdziwej tożsamości komunikujących się serwerów i przeglądarek WWW.

SSL opracowany przez Netscape Communications, funkcjonuje w oparciu na protokole transmisji połączeniowej TCP, ograniczając się do zakresu warstwy transportowej modelu komunikacyjnego TCP/IP, co pozwala na zastosowanie jej do ochrony innych usług Internetu, np. FTP, Telnet.

Filtry pakietów

Technika ta jest najprostszą formą firewalla. Polega ona na kasowaniu wszystkich pakietów, które zawierają obce adresy, tzn. te, które nie zostały umieszczone przez administratora w tablicy źródeł i ujść. Tablice te utrzymuje się dla obu kierunków współpracy, to znaczy do i z Internetu [rys 7].

Gateway poziomu aplikacji

Gateway poziomu aplikacji posiada dodatkową warstwę ochrony zwiększającą bezpieczeństwo połączeń pomiędzy Intranetem i Internetem. Wyróżnić można trzy główne elementy:

– węzeł Gateway,

– dwie ściany ogniowe [rys. 8].

Konfiguracja ta pozwala na swobodny przepływ poczty elektronicznej pomiędzy Internetem i siecią lokalną, transfer plików, a operacja zdalnego logowania odbywa się w specjalny sposób.

Tunele szyfrujące

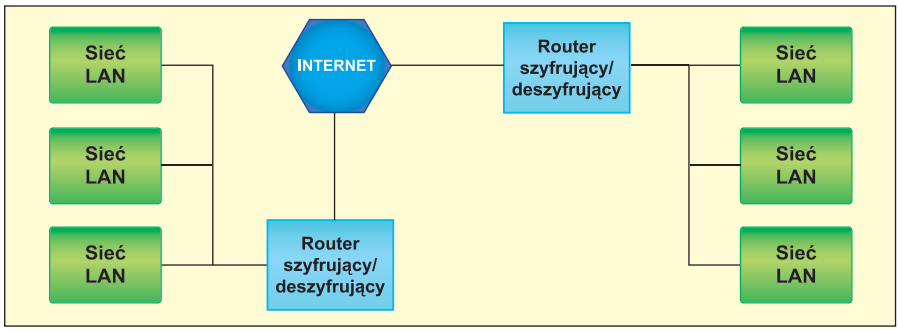
Kolejna metodą ochrony jest szyfrowanie wiadomości opuszczających sieć i deszyfrowanie wiadomości wchodzących z zewnątrz. Klucze wymagane w procesie szyfrowania i deszyfrowania znane są jedynie autoryzowanym użytkownikom. Dodatkową zaletą takiego rozwiązania jest utrudniona w znaczny sposób możliwość podsłuchania. Operacji szyfrowania i deszyfrowania dokonują routery przyłączone bezpośrednio do sieci Internet [rys. 9].

Aplikacja firewall

Firewall-1, jest zintegrowanym rozwiązaniem umożliwiającym zastosowanie większość z wcześniej omawianych sposobów zabezpieczeń pozwalającym na bieżące monitorowanie wszystkich otwartych sesji komunikacji, niezależnie od tego, czy transmisja danych prowadzona jest w oparciu na komunikacji połączeniowej TCP, czy bezpołączeniowo UDP. Zaimplementowany przejrzysty interfejs graficzny pozwala w znacznym stopniu usprawnić proces wdrażania i nadzorowania realizacji przyjętej strategii ochrony.

Zestaw potencjalnych możliwości Firewall-1 obejmuje:

– filtrację pakietów (przeciwdziałanie „spoofing"),
– aplikacje pośredniczące (prowadzenie identyfikacji, kontroli tożsamości, kontroli uprawnień),
– translację adresów internetowych (ukrywanie wewnętrznych adresów IP),
– szyfrowanie i uwierzytelnianie, tworzenie wirtualnych sieci prywatnych VPN.



Rys. 9. Tunel szyfrujący

Testy penetracyjne

Inaczej testy bezpieczeństwa systemów informatycznych. Zadaniem ich jest ukazanie faktycznych oraz potencjalnych błędów w archiekturze, oprogramowaniu oraz użytkowaniu sieci komputerowych.

Test polega na dokonaniu serii kontrolowanych ataków na testowany system symulując w ten sposób rzeczywistą próbę naruszenia bezpieczeństwa i stabilności sieci. Do przeprowadzenia ataków wykorzystuje się zarówno ogólnie dostępne techniki i programy, jak i specjalistyczne narzędzia stworzone przez ekspertów specjalizujących się w tego typu usługach.

Zakończenie

Od prowadzonej strategii ochrony w lokalnych sieciach komputerowych zależy bezpieczeństwo wszystkich zawartych w nich dóbr, takich jak dane o klientach, wyniki finansowe, projekty inżynierskie związane z prowadzoną działalnością.

Ochrona ta powinna podlegać ciągłemu nadzorowi, tak aby nie dopuścić do utraty poufności gromadzonych czy też przesyłanych informacji.

Zrozumiałą staje się teza, iż tylko aktywna i systematyczna kontrola sieci jest w stanie zapewnić jej bezpieczeństwo.

Cezary Kukuć
CMA

Literatura:

[1] Jacek Jarmakiewicz, *Sieci Teleinformatyczne*, Wyższa Szkoła Informatyki Stosowanej i Zarządzania Warszawa 2001
[2] *Zagrożenia z Sieci*, CMS – Centrum Monitorowania Sieci