Podstawy bezpieczeństwa sieciowego

Dariusz Chaładyniak
Warszawska Wyższa Szkoła Informatyki
dchalad@wwsi.edu.pl

Streszczenie

Bezpieczeństwo danych przesyłanych w sieciach komputerowych jest jednym z najważniejszych zadań współczesnej teleinformatyki. Wykład przedstawia podstawowe rodzaje złośliwego oprogramowania (wirusy, trojany, robaki) oraz wybrane programy antywirusowe (skanery, monitory, szczepionki). Opisano także najczęściej spotykane metody ataków na systemy i sieci komputerowe (zewnętrzne, wewnętrzne, tradycyjne, rozproszone) oraz ich rodzaje (DoS, DDoS, phishing, spam). Przedstawione będą ponadto wybrane narzędzia i aplikacje do zabezpieczania danych, działanie systemów wykrywania włamań oraz metody przeciwdziałania atakom sieciowym z wykorzystaniem zapór ogniowych (sprzętowych i programowych).

Spis treści

1 ZŁOŚLIWE OPROGRAMOWANIE

1.1 RODZAJE ZŁOŚLIWEGO OPROGRAMOWANIA

Złośliwe oprogramowanie (ang. *malicious software*) to programy, które muszą zostać wprowadzone do komputera użytkownika. Mogą one uszkodzić system, zniszczyć dane, a także uniemożliwić dostęp do sieci, systemów lub usług. Mogą one też wykraść dane lub informacje osobiste ze stacji użytkownika i przesłać je samoczynnie do przestępców. W większości przypadków umieją same się replikować i rozprzestrzeniać na inne hosty dołączone do sieci. Czasem techniki te są używane w połączeniu z socjotechniką, aby oszukać nieostrożnego użytkownika, by ten nieświadomie uruchomił taki atak. Przykładami złośliwego oprogramowania są wirusy, robaki oraz konie trojańskie.

Wirus jest programem, który działa i rozprzestrzenia się przez modyfikowanie innych programów lub plików. Wirus nie może uruchomić się sam, musi zostać uaktywniony. Po uaktywnieniu, może nie robić nic poza replikacją i rozprzestrzenianiem się. Nawet prosty typ wirusa jest niebezpieczny, gdyż może szybko zużyć całą dostępną pamięć komputera i doprowadzić system do zatrzymania. Groźniejszy wirus, przed rozprzestrzenieniem się, może usunąć lub uszkodzić pliki. Wirusy mogą być przenoszone przez załączniki poczty elektronicznej, pobierane pliki, komunikatory, a także dyskietki, płyty CD/DVD lub urządzenia USB.

Rodzaje wirusów komputerowych:

1. **Pasożytnicze** – wykorzystują swoje ofiary do transportu;
2. **Polimorficzne** – mogą zmieniać swój kod;
3. **Wirusy plików wsadowych** – wykorzystują do transportu pliki z rozszerzeniem .bat.

Najbardziej znane wirusy to: Chernobyl (CIH), Christmas Tree.

Robak (ang. *worm*) jest podobny do wirusa, lecz w odróżnieniu od niego nie musi dołączać się do istniejącego programu. Robak używa sieci do rozsyłania swych kopii do podłączonych hostów. Robaki mogą działać samodzielnie i szybko się rozprzestrzeniać. Nie wymagają aktywacji czy ludzkiej interwencji. Samorozprzestrzeniające się robaki sieciowe są o wiele groźniejsze niż pojedynczy wirus, gdyż mogą szybko zainfekować duże obszary Internetu. Najbardziej znane robaki to: I Love You, Melissa, Mydoom, Netsky.

Koń trojański (ang. *trojan horse*), zwany również **trojanem**, jest programem, który nie replikuje się samodzielnie. Wygląda jak zwykły program, lecz w rzeczywistości jest narzędziem ataku. Idea działania konia trojańskiego polega na zmyleniu użytkownika, by ten uruchomił jego kod myśląc, że uruchamia bezpieczny program. Koń trojański jest zwykle mało szkodliwy, ale może zupełnie zniszczyć zawartość twardego dysku. Trojany często tworzą furtkę dla hakerów – pełny dostęp do zasobów komputera. Najbardziej znane trojany to: Connect4, Flatley Trojan, Poison Ivy.

Bomba logiczna (ang. *logical bomb*), w odróżnieniu od konia trojańskiego, nie uruchamia ukrytego złośliwego oprogramowania od razu tylko w odpowiednim czasie (np. po zajściu określonego zdarzenia lub po kilkukrotnym uruchomieniu wybranej aplikacji).

Exploit jest programem wykorzystującym błędy programistyczne i przejmującym kontrolę nad działaniem procesu.

Keylogger jest oprogramowaniem, mającym na celu wykradanie haseł poprzez przejęcie kontroli nad obsługą klawiatury.

Ransomware (ang. *ransom* – okup) jest aplikacją wnikającą do atakowanego komputera, a następnie szyfrującą dane jego właściciela. Perfidia tego złośliwego oprogramowania polega na zostawieniu odpowiedniej notatki z instrukcją, co musi zrobić właściciel zainfekowanego komputera, aby odzyskać dane.

Rootkit jest programem ułatwiającym włamanie do systemu komputerowego poprzez ukrycie niebezpiecznych plików i procesów mających kontrolę nad systemem. Wykrycie takiego programu w zainfekowanym komputerze jest bardzo trudne, gdyż jest on w stanie kontrolować pracę specjalistycznych narzędzi do jego wykrywania. Najbardziej znane to: Hacker Defender, CD Sony Rootkit.

Spyware to złośliwe oprogramowanie mające na celu szpiegowanie działań użytkownika komputera. Zadaniem spyware jest gromadzenie informacji o użytkowniku (adresy stron internetowych odwiedzanych przez użytkownika, dane osobowe, numery kart kredytowych i płatniczych, hasła, adresy e-mail). Najbardziej znane spyware to: Gator, Cydoor, Save Now.

Stealware jest oprogramowaniem okradającym nieświadomego użytkownika poprzez śledzenie jego działań. Instalacja takiego programu odbywa się bez wiedzy i zgody użytkownika za pomocą odpowiednio spreparowanych wirusów komputerowych, robaków lub stron WWW wykorzystujących błędy i luki w przeglądarkach internetowych. Stealware w przypadku stwierdzenia próby płatności przez Internet podmienia numer konta, na które zostaną wpłacone pieniądze.

1.2 RODZAJE PROGRAMÓW ANTYWIRUSOWYCH

Poniżej przedstawiamy wybrane rodzaje programów antywirusowych.

Skaner (ang. *scanner*) należy do najstarszych i najprostszych sposobów ochrony przed wirusami komputerowymi. Zasada działania skanera polega na wyszukiwaniu pewnej sekwencji bajtów w zadanym ciągu danych. Skaner jest tym skuteczniejszy, im wirus zawiera w sobie bardziej charakterystyczny napis lub ciąg bajtów.

Monitor (ang. *resident monitor*) to oprogramowanie antywirusowe zainstalowane w systemie operacyjnym jako program rezydentny. Skuteczność monitora zależy od tego, czy przejął on kontrolę nad systemem przed działaniem wirusa, czy po jego działaniu oraz od tego, jak głęboko wnika on w system operacyjny.

Szczepionka (ang. *disinfector*) jest oprogramowaniem antywirusowym, działającym przeciwko konkretnym infekcjom. Po wykryciu wirusa i poddaniu odpowiedniej analizie jego kodu można zdefiniować pewne właściwości umożliwiające przygotowanie właściwej szczepionki.

Program zliczający sumy kontrolne (ang. *integrity checker*) przy pierwszym uruchomieniu dokonuje odpowiednich obliczeń dla plików zgromadzonych na dysku, a następnie wykorzystuje te dane, aby porównać z bieżąco wyliczoną sumą kontrolną i na tej podstawie stwierdzić ewentualną obecność wirusa.

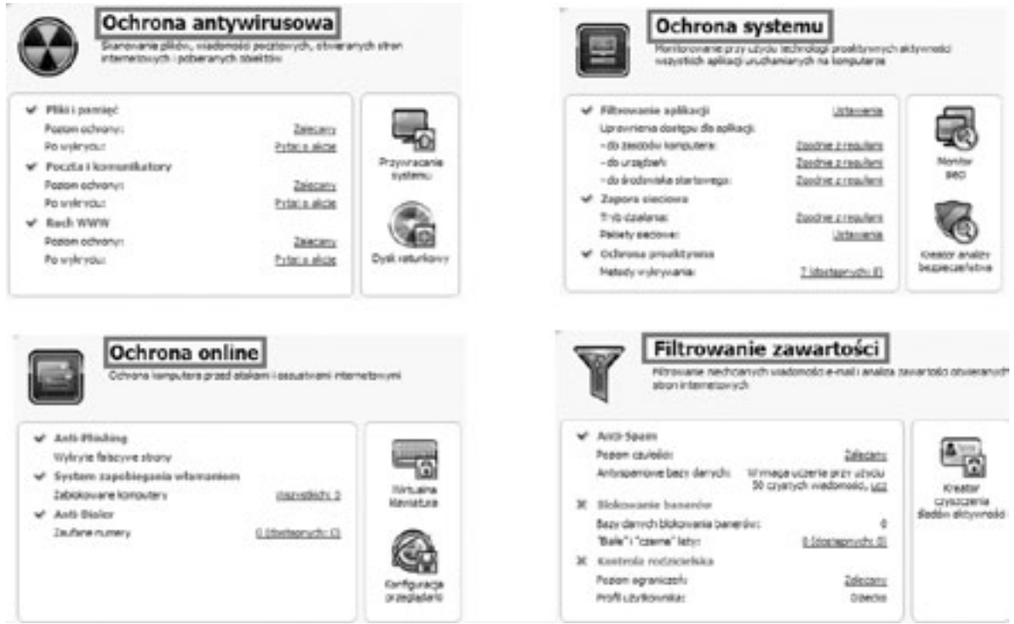
1.3 PROFILAKTYKA ANTYWIRUSOWA

Jedną z najlepszych metod zabezpieczenia się przed wirusami komputerowymi jest posiadanie najnowszego oprogramowania do ich zwalczania. Na rysunku 1 pokazano zakładkę Centrum zabezpieczeń w Panelu sterowania z włączoną funkcją ochrony przed wirusami.

Rysunek 1.
Zakładka Centrum zabezpieczeń w systemie Windows XP z informacją o włączonej ochronie przed wirusami

Jednym z najpopularniejszych i najbardziej skutecznych programów antywirusowych jest Kaspersky Internet Security 2009 (rys. 2). Aplikacja ta kompleksowo chroni komputer przed złośliwym oprogramowaniem, oszustwami internetowymi oraz nieautoryzowanym dostępem. Prowadzi ochronę antywirusową (skanowanie plików, wiadomości pocztowych, otwieranych stron internetowych i pobieranych obiektów), ochronę systemu (filtrowanie aplikacji, zapora sieciowa, ochrona proaktywna), ochronę *on-line* (ochrona komputera przed atakami i oszustwami internetowymi), a także filtrowanie zawartości (filtrowanie niechcianych wiadomości e-mail, analiza zawartości otwieranych stron internetowych) – patrz rysunek 3.

Rysunek 2.
Program antywirusowy Kaspersky Internet Security 2009



Rysunek 3.
Funkcje programu Kaspersky Internet Security 2009

2 WYBRANE ATAKI NA SIECI TELEINFORMATYCZNE

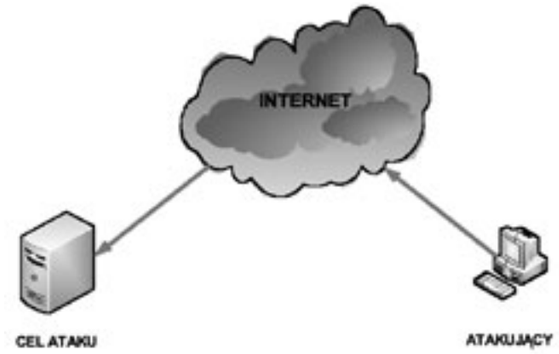
2.1 SPOSOBY ATAKOWANIA SIECI

Sieć można atakować na wiele sposobów:

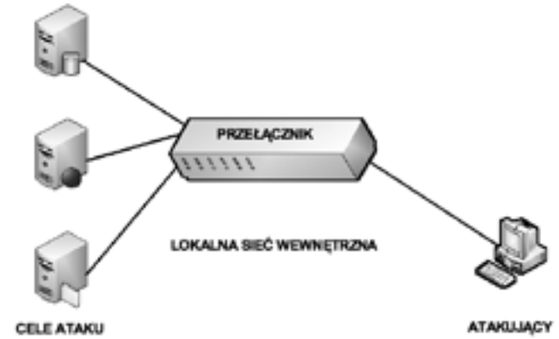
- atak zewnętrzny;
- atak wewnętrzny;
- atak tradycyjny;
- atak przy pomocy węzłów pośredniczących;
- atak rozproszony.

Atak zewnętrzny (rys. 4) jest powodowany przez osoby, które nie pracują w danej organizacji. Atakujący z zewnątrz toruje sobie drogę do sieci głównie przez Internet, łącza bezprzewodowe lub usługi wdzwaniane.

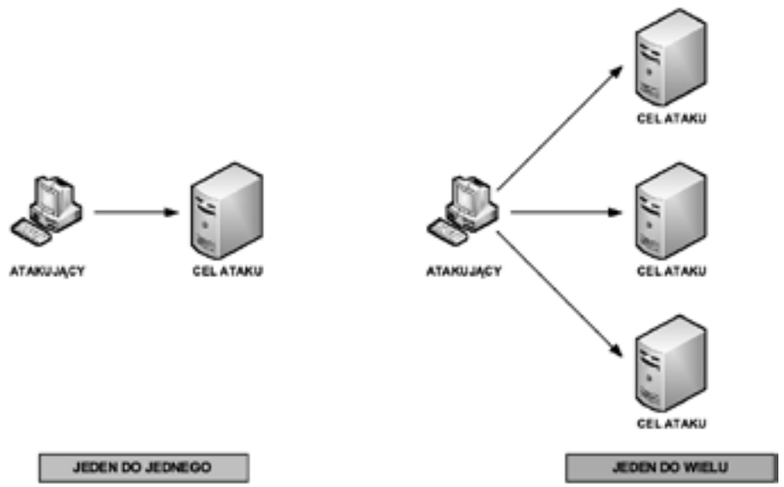
Atak wewnętrzny (rys. 5) może przeprowadzić ktoś, kto ma dostęp do sieci, czyli posiada konto lub ma dostęp fizyczny. Atakujący przeważnie zna ludzi oraz politykę wewnętrzną firmy. Nie wszystkie wewnętrzne ataki są celowe. W niektórych przypadkach zagrożenie wewnętrzne może powodować niefrasobliwy pracownik, który ściągnie i uruchomi wirusa, a następnie nieświadomie wprowadzi go do wnętrza sieci. Większość firm wydaje znaczące sumy na ochronę przed zewnętrznymi atakami, mimo iż gros zagrożeń pochodzi ze źródeł wewnętrznych. Jak podają statystyki, dostęp z wewnątrz i nadużycie systemów komputerowych stanowi ok. 70% zgłoszonych naruszeń bezpieczeństwa.



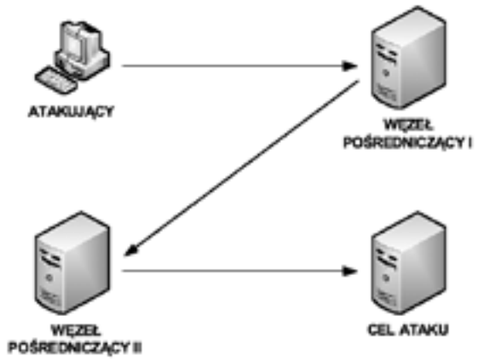
Rysunek 4.
Przykład ataku z sieci zewnętrznej



Rysunek 5.
Przykład ataku z sieci wewnętrznej



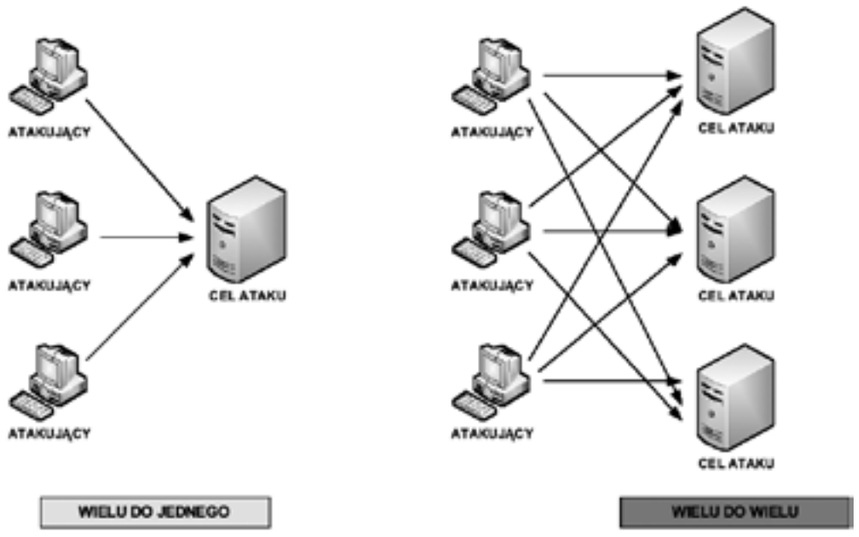
Rysunek 6.
Przykłady ataków tradycyjnych



Rysunek 7.
Przykład ataku przy udziale węzłów pośredniczących

Atak tradycyjny (rys. 6) polega na atakowaniu z jednego komputera jednego lub wielu hostów sieciowych.

Często zdarza się, że włamywacze nie atakują bezpośrednio, a korzystają z komputerów ofiar dla ukrycia prawdziwego źródła ataku oraz utrudnienia ich odnalezienia. Jak widać na rysunku 7, intruz korzysta z kilku węzłów pośredniczących tak, aby atakowany obiekt zinterpretował je jako źródła ataków.



Rysunek 8.
Przykłady ataków rozproszonych

Atak rozproszony (rys. 8) polega na zainicjowaniu przez atakującego wielu jednoczesnych ataków na jeden lub wiele celów. Zwykle następuje on w dwóch fazach. Początkowo atakujący musi przygotować węzły, z których atak taki mógłby być przeprowadzony. Polega to na ich znalezieniu i zainstalowaniu oprogramowania, które będzie realizowało właściwą fazę ataku rozproszonego. Cechą charakterystyczną drugiej fazy jest wysyłanie pakietów przez atakującego z węzłów pośredniczących, a nie z hosta atakującego. Ataki rozproszone

przynoszą atakującemu korzyści w postaci utajenia źródła ataku, zmasowanej siły ataku, poszerzenia bazy wiedzy na temat atakowanego celu i wreszcie trudności w jego zatrzymaniu.

2.2 RODZAJE WŁAMAŃ SIECIOWYCH

Po uzyskaniu dostępu do sieci haker może powodować następujące zagrożenia (rys. 9):

1. **Kradzież informacji** – włamanie do komputera w celu uzyskania poufnych informacji. Skradzione informacje mogą zostać użyte do różnych celów lub sprzedane.
2. **Kradzież tożsamości** – forma kradzieży, w której przedmiotem kradzieży stają się informacje osobiste, mająca na celu przejęcie czyjejś tożsamości. Używając takich informacji, włamywacz może uzyskać dokumenty, wyłudzić kredyt lub dokonać zakupów w sieci. Jest to coraz powszechniejsza forma włamania sieciowego powodująca miliardowe straty.
3. **Utrata i zmiana danych** – włamanie do komputera, w celu zniszczenia lub dokonania manipulacji danych. Przykłady utraty danych to: wysłanie wirusa formatującego dysk twardy ofiary lub dokonanie zmiany np. ceny danego towaru.
4. **Blokada usług** – uniemożliwienie świadczenia usług sieciowych.

Rysunek 9.
Wybrane rodzaje włamań do sieci komputerowych

2.3 RODZAJE ATAKÓW SIECIOWYCH

Spam

Niechciane masowe przesyłki e-mail to kolejny dokuczliwy produkt wykorzystujący naszą potrzebę elektronicznej komunikacji. Niektórzy handlowcy nie tracą czasu na ukierunkowanie reklamy. Chcą wysyłać reklamy do jak największej liczby użytkowników w nadziei, że ktoś będzie zainteresowany ich produktem lub usługą. Takie szeroko dystrybuowane podejście do marketingu w Internecie określane jest mianem **spamu**.

Spam stanowi poważne zagrożenie, które może przeciążyć sieci dostawców usług sieciowych, serwery pocztowe oraz komputery użytkowników. Osoba lub organizacja odpowiedzialna za wysyłanie spamu jest nazywana **spamerem**. Spamerzy zwykle wykorzystują niezabezpieczone serwery pocztowe do rozsyłania poczty. Mogą też użyć technik hakerskich, takich jak: wirusy, robaki i konie trojańskie do przejęcia kontroli nad domowymi komputerami. Komputery te są wówczas używane do wysyłania spamu bez wiedzy właściciela. Spam może być rozsyłany przez pocztę elektroniczną lub, przez komunikatory sieciowe.

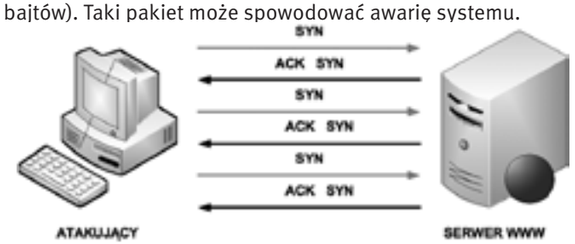
Atak DoS

Ataki DoS (ang. *Denial of Service*) są prowadzone na pojedyncze komputery lub grupy komputerów i mają na celu uniemożliwienie korzystania z usług. Celem ataku DoS mogą być systemy operacyjne, serwery, routery i łącza sieciowe. Główne cele ataków DoS to:

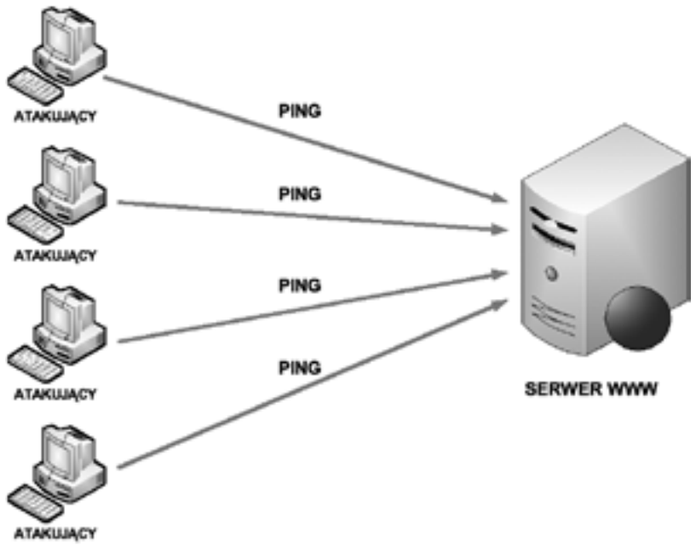
- Zalanie systemu (lub sieci) ruchem, aby zablokować ruch pochodzący od użytkowników.
- Uszkodzenie połączenia pomiędzy klientem i serwerem, aby uniemożliwić dostęp do usługi.

Istnieje kilka typów ataków DoS. Administratorzy odpowiedzialni za bezpieczeństwo muszą być świadomi ich istnienia i wiedzieć, jak się przed nimi uchronić. Dwa podstawowe przykłady ataków DoS to:

1. **Zalewanie SYN** (synchroniczne) – zalewanie serwera pakietami rozpoczynającymi nawiązanie połączenia. Pakiety te zawierają nieprawidłowy źródłowy adres IP. Serwer nie odpowiada na żądania użytkowników, ponieważ jest zajęty generowaniem odpowiedzi na fałszywe zapytania (rys. 10).
2. **Ping śmierci** (ang. *Ping of death*) – do urządzenia sieciowego wysyłany jest pakiet o rozmiarze większym niż maksymalny (65 535 bajtów). Taki pakiet może spowodować awarię systemu.



Rysunek 10.
Przykład ataku typu DoS



Rysunek 11.
Przykład ataku typu DDoS

Atak DDoS

Atak DDoS (ang. *Distributed Denial od Service*) jest odmianą ataku DoS, ale o wiele bardziej wyrafinowaną i potencjalnie bardziej szkodliwą. Został stworzony, aby nasycić sieć bezużytecznymi danymi. DDoS działa na znacznie większą skalę niż ataki DoS. Zwykle atakuje setki lub tysiące miejsc jednocześnie. Tymi miejscami mogą być komputery zainfekowane wcześniej kodem DDoS. Służą do tego najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego złośliwego oprogramowania. Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej ilości żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu (rys. 11).

Phishing

Phishing jest techniką wyłudzania poufnych informacji poprzez podszywanie się pod osobę pracującą w atakowanej organizacji, np. w banku. Atakujący zwykle kontaktuje się za pomocą poczty elektronicznej. Może poprosić o weryfikację informacji (np. hasła, nazwy użytkownika), by rzekomo zabezpieczyć ofiarę przed groźnymi konsekwencjami.

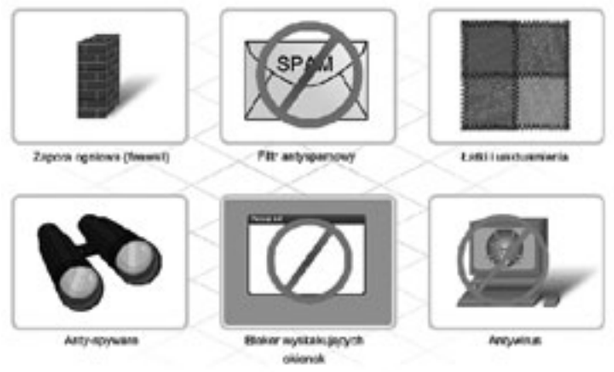
3 WYBRANE METODY BEZPIECZEŃSTWA SIECIOWEGO

3.1 NARZĘDZIA I APLIKACJE DO ZABEZPIECZANIA SIECI

Polityka bezpieczeństwa powinna być centralnym punktem procesów zabezpieczania, monitorowania, testowania i ulepszania sieci. Tę politykę realizują procedury bezpieczeństwa, które określają procesy konfiguracji, logowania, audytu oraz obsługi hostów i urządzeń sieciowych. Mogą definiować kroki prewencyjne zmniejszające ryzyko jednocześnie informując, jak radzić sobie po stwierdzeniu naruszenia zasad bezpieczeństwa. Procedury te mogą zawierać proste zadania, takie jak zarządzanie i aktualizacja oprogramowania, ale też złożone implementacje zapór ogniowych i systemów wykrywania włamań.

Przykłady narzędzi i aplikacji używanych do zabezpieczania sieci (rys. 12):

1. **Zapora ogniowa** (ang. *firewall*) – sprzętowe lub programowe narzędzie bezpieczeństwa, które kontroluje ruch do i z sieci.
2. **Bloker spamu** – oprogramowanie zainstalowane na serwerze lub komputerze użytkownika, identyfikujące i usuwające niechciane wiadomości.
3. **Łatki i aktualizacje** – oprogramowanie dodane do systemu lub aplikacji naprawiające luki w bezpieczeństwie lub dodające użyteczną funkcjonalność.
4. **Ochrona przed spyware** – oprogramowanie zainstalowane na stacji użytkownika do wykrywania i usuwania spyware i adware.
5. **Blokery wyskakujących okienek** – oprogramowanie zainstalowane na komputerze użytkownika do zabezpieczania przed wyskakiwaniem okienek z reklamami.
6. **Ochrona przed wirusami** – oprogramowanie zainstalowane na komputerze użytkownika lub serwerze, wykrywające i usuwające wirusy, robaki oraz konie trojańskie z plików i wiadomości e-mail.

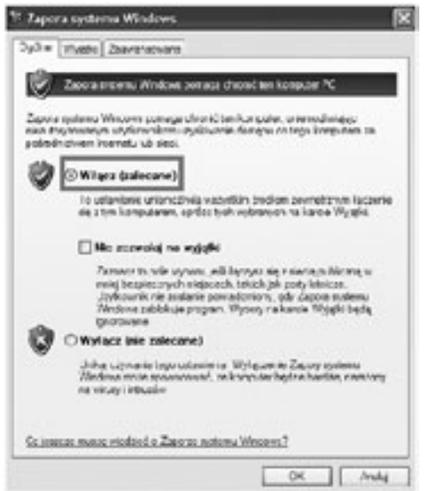


Rysunek 12.
Wybrane narzędzia i aplikacje do zabezpieczania sieci komputerowych

3.2 INSTALACJA ZAPORY OGNIOWEJ

Jedną ze skuteczniejszych metod zabezpieczenia sieci komputerowej przed atakiem jest włączenie i skonfigurowanie zapory ogniowej. Na rysunku 13 pokazano zakładkę Centrum zabezpieczeń w Panelu sterowania z włączoną funkcją zapory ogniowej. Aby skonfigurować zaporę ogniową w systemie operacyjnym, należy kliknąć na opcji Zapora systemu Windows.

Rysunek 13.
Zakładka Centrum zabezpieczeń w systemie Windows XP z informacją o włączonej zaporze ogniowej

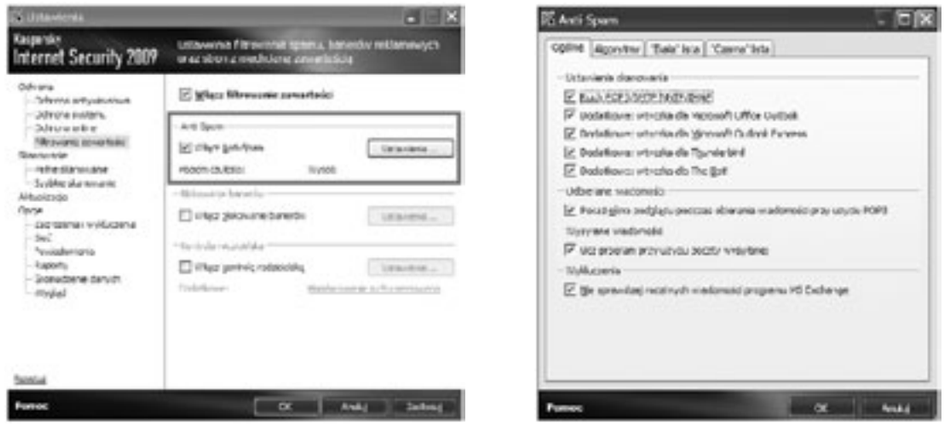


Rysunek 14.
Ustawienia zapory ogniowej

Zapora ogniowa chroni komputer przed nieautoryzowanym dostępem z sieci. Włączenie zapory (rys. 14) uniemożliwia połączenie się z tym komputerem z zewnątrz poza wybranymi wyjątkami (rys. 15).

Na rysunku 16 przedstawiono ustawienie filtrowania spamu w programie Kaspersky Internet Security 2009.

Rysunek 15.
Zaznaczenie programów i usług nieblokowanych przez zaporę ogniową



Rysunek 16.
Ustawienia filtrowania spamu w programie Kaspersky Internet Security 2009

Do głównych narzędzi polepszających zabezpieczenia sieci komputerowych jest przeprowadzanie automatycznych aktualizacji. Rysunek 17 pokazuje zakładkę Centrum zabezpieczeń w Panelu sterowania z włączoną funkcją Aktualizacje automatyczne. Po kliknięciu na zaznaczonej opcji ukazuje się obraz pokazany na rysunku 18.

Rysunek 17.
Zakładka Centrum zabezpieczeń w systemie Windows XP z informacją o włączonych automatycznych aktualizacjach

Rysunek 18.
Ustawienia automatycznych aktualizacji

Rysunek 19.
Kreator kopii zapasowej

Jedną z głównych gwarancji bezpieczeństwa danych jest ich regularne archiwizowanie, które można wykonywać na trzy sposoby:

1. **Kopia pełna** (ang. *full backup*) – polega na skopiowaniu wszystkich wybranych plików i oznaczeniu każdego z nich jako zarchiwizowany. Kopie pełne są najłatwiejsze w użyciu podczas odzyskiwania plików, ponieważ wymagają jedynie posiadania najświeższego pliku. Wykonywanie kopii pełnych zajmuje jednak najwięcej przestrzeni na nośnikach (i zazwyczaj czasu), ponieważ kopiowany jest każdy plik, niezależnie od tego, czy został zmieniony od czasu tworzenia ostatniej kopii zapasowej.
2. **Kopia przyrostowa** (ang. *incremental backup*) – polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii przyrostowej lub pełnej oraz na oznaczeniu ich jako zarchiwizowane. Przed utworzeniem pierwszej kopii przyrostowej powinno się utworzyć pełną kopię systemu. Jeżeli korzysta się z kombinacji kopii pełnych oraz przyrostowych, to do odtworzenia danych niezbędne są, w chronologicznym porządku: ostatnio utworzona kopia pełna oraz wszystkie kolejne kopie przyrostowe.
3. **Kopia różnicowa** (ang. *differential backup*) – polega na kopiowaniu jedynie tych plików, które zostały utworzone lub zmienione od czasu utworzenia ostatniej kopii pełnej. Podczas wykonywania kopii różnicowej kopiowane pliki nie są oznaczane jako zarchiwizowane. Przed utworzeniem pierwszej kopii różnicowej zalecane jest wykonanie pełnej kopii. Jeżeli korzysta się z kombinacji kopii pełnych oraz różnicowych, to do odtworzenia danych niezbędne są: ostatnia kopia pełna oraz ostatnia kopia różnicowa.

4 SYSTEMY WYKRYWANIA INTRUZÓW (WŁAMAŃ)

4.1 SYSTEMY IDS

Zadaniem **systemu wykrywania intruzów** (ang. *Intrusion Detection System,* IDS) jest identyfikacja zagrożenia w sieci komputerowej. Podstawą wykrywania włamań jest monitorowanie ruchu w sieci. Systemy wykrywania włamań działają w oparciu o informacje odnoszące się do aktywności chronionego systemu – współczesne systemy IDS analizują w czasie rzeczywistym aktywność w sieci.

Włamanie do systemu najczęściej przebiega w dwóch etapach:

- Etap pierwszy – próba penetracji systemu będącego celem ataku. Intruz usiłuje znaleźć lukę w systemie (na przykład próbuje skanować porty), umożliwiającą wtargnięcie do systemu poprzez ominięcie systemów zabezpieczających.
- Etap drugi – wtargnięcie do systemu. Jednocześnie odbywa się próba zamaskowania obecności intruza poprzez odpowiednie zmiany w logach systemowych. Włamywacz podejmuje również próby modyfikacji narzędzi systemowych tak, by uniemożliwić swoje wykrycie.

Systemy IDS analizują procesy zachodzące w newralgicznych obszarach sieci objętej ochroną. Umożliwiają więc wykrycie niepożądanych zajść podczas próby włamania oraz po udanym włamaniu – jest to bardzo ważne ze względów bezpieczeństwa, ponieważ IDS działa dwufazowo – nawet jeżeli intruz zdoła włamać się do systemu, nadal może zostać wykryty i unieszkodliwiony, mimo usilnego zacierania śladów swojej działalności.

Systemy IDS korzystają z czterech podstawowych metod, dzięki którym możliwe jest zidentyfikowanie intruza wewnątrz chronionej sieci:

1. **Dopasowywanie wzorców** – jest to najprostsza metoda detekcji intruza; pojedynczy pakiety porównywany jest z listą reguł. Jeśli któryś z warunków jest spełniony, to jest uruchamiany alarm.
2. **Kontekstowe dopasowywanie wzorców** – w kontekstowym dopasowywaniu pakietu, system bierze pod uwagę kontekst każdego pakietu. Śledzi połączenia, dokonuje łączenia fragmentowanych pakietów.

3. **Analiza heurystyczna** – wykorzystuje algorytmy do identyfikacji niepożądanego działania. Algorytmy te są zwykle statystyczną oceną normalnego ruchu sieciowego. Przykładowo, algorytm stwierdzający skanowanie portów wykazuje, że takie wydarzenie miało miejsce, jeżeli z jednego adresu w krótkim czasie nastąpi próba połączeń z wieloma portami.
4. **Analiza anomalii** – sygnatury anomalii starają się wykryć ruch sieciowy, który odbiega od normy. Największym problemem jest określenie stanu uważanego za normalny.

Mimo ciągłego rozwoju systemów IDS napotykają one na liczne przeszkody, które zniekształcają prawidłowe działanie oprogramowania:

1. Mnogość aplikacji – w przypadku ataku na konkretną aplikację, polegającym na podawaniu jej nietypowych danych, system musi „rozumieć" protokół, którego dana aplikacja używa. Protokołów sieciowych jest bardzo wiele i system IDS na ogół nie zna ich wszystkich, a tylko pewien ich podzbiór. Jest to wykorzystywane przy próbach ataku na sieć chronioną przez IDS.
2. Defragmentacja pakietów – wykrycie ataku rozłożonego na kilka pakietów wymaga monitorowania przebiegu sesji. Takie działanie pochłania jednak część zasobów komputerowych: pamięć i czas.
3. Fałszywe alarmy.
4. Ograniczenia zasobów – zajęcie wszystkich zasobów sensora jest wykorzystywane do ataków na sieci chronione przez IDS.

Istnieją cztery główne rodzaje ataków, które systemy klasy IDS są w stanie rozpoznać:

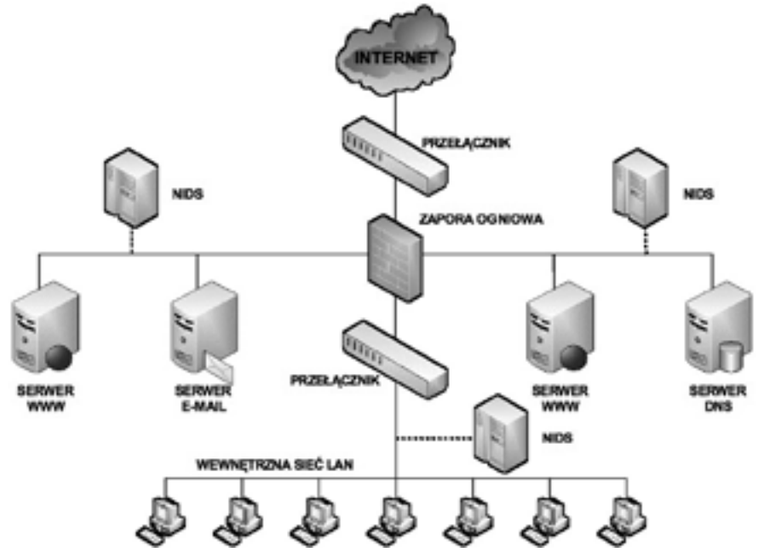
1. Nieautoryzowany dostęp do zasobów – najbardziej liczna grupa ataków zawierająca w sobie między innymi łamanie haseł dostępowych, używanie koni trojańskich oraz podszywanie się.
2. Nieuprawniona modyfikacja zasobów – to nieuprawnione modyfikacje, kasowanie danych oraz generowanie nieuprawnionych transmisji danych.
3. Blokowanie usług – przede wszystkim ataki typu DoS/DDoS.
4. Ataki zorientowane na aplikacje – ataki wykorzystujące błędy oraz luki zawarte w aplikacjach.

4.2 RODZAJE SYSTEMÓW IDS

Działanie pierwszych systemów do wykrywania włamań polegało przede wszystkim na szczegółowej analizie wystąpienia niebezpiecznego zdarzenia. Współczesne aplikacje IDS wykonują dodatkowo monitorowanie sieci oraz wykrywanie i reagowanie w czasie rzeczywistym na nieautoryzowane działania w sieci. Wyróżnia się trzy główne rodzaje systemów IDS:

1. **NIDS** (ang. *Network Intrusion Detection System,* sieciowy system wykrywania intruzów) – rozwiązania sprzętowe lub programowe śledzące sieć.
2. **HIDS** (ang. *Host Intrusion Detection System,* hostowy system wykrywania intruzów) – aplikacje instalowane na chronionych serwerach usług sieciowych.
3. **NNIDS** (ang. *Network Node Intrusion Detection System,* hybrydowy system wykrywania intruzów) – rozwiązania hybrydowe.

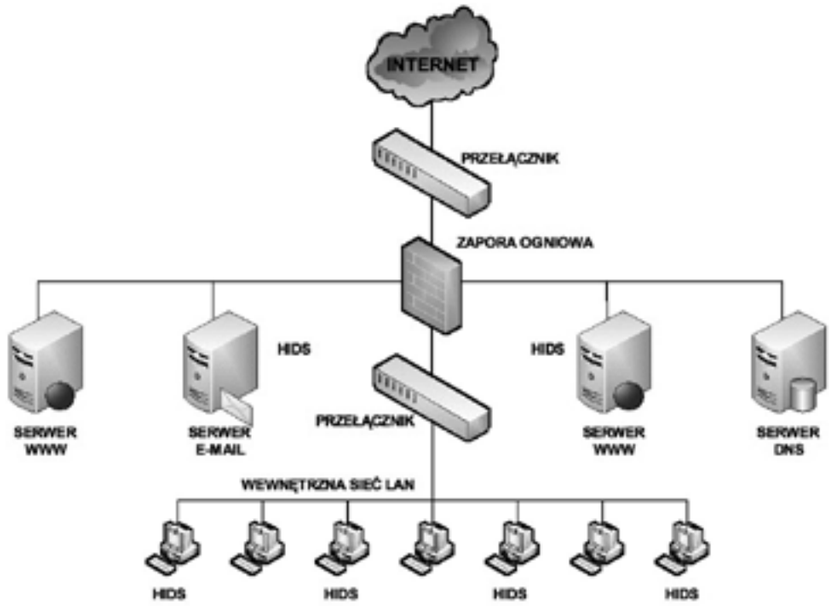
Na rysunku 20 pokazany jest schemat sieciowego systemu wykrywania intruzów (NIDS). Takie rozwiązanie umożliwia skuteczne monitorowanie wydzielonego segmentu sieci. System NIDS może podsłuchiwać wszelką komunikację prowadzoną w tej sieci. To rozwiązanie jest nastawione na ochronę publicznie dostępnych serwerów zlokalizowanych w podsieciach stref zdemilitaryzowanych (patrz p. 5.2).



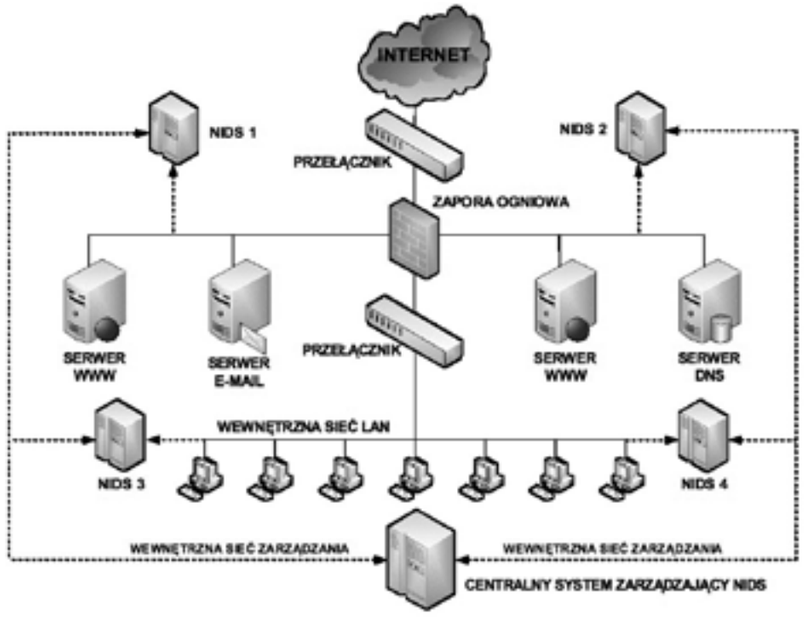
Rysunek 20.
Schemat systemu wykrywania włamań typu NIDS

Schemat hostowego systemu wykrywania intruzów (HIDS) jest przedstawiony na rysunku 21. Podstawowa różnica między systemami HIDS a NIDS polega na tym, że w pierwszym przypadku chroniony jest tylko komputer, na którym system rezyduje. Ponadto system HIDS można uruchamiać na zaporach ogniowych, zabezpieczając je w ten sposób.

Rysunek 22 pokazuje hybrydowy system wykrywania intruzów (NNIDS), składający się z czterech sensorów i centralnego systemu zarządzającego. Standardowo systemy NNIDS funkcjonują w ramach architektury przeznaczonej do obsługi zarządzania i badania sieci. Sensory wykrywania włamań systemów NIDS są zlokalizowane zdalnie w odpowiednich miejscach i składają raporty do centralnego systemu zarządzania NIDS. Dzienniki ataków są co jakiś czas dostarczane do systemu zarządzającego i mogą być tam przechowywane w centralnej bazie danych. Z kolei nowe sygnatury ataków mogą być ładowane do systemów-sensorów. Zgodnie z przedstawionym schematem, sensory NIDS1 i NIDS2 operują w cichym trybie odbierania i chronią serwery dostępu publicznego. Natomiast sensory NIDS3 i NIDS4 chronią systemy hostów znajdujących się wewnątrz sieci zaufanej.



Rysunek 21.
Schemat systemu wykrywania włamań typu HIDS



Rysunek 22.
Schemat systemu wykrywania włamań typu NNIDS

5 DZIAŁANIE ZAPÓR OGNIOWYCH

5.1 PODSTAWOWE FUNKCJE ZAPÓR OGNIOWYCH

Zapora ogniowa jest jednym z najefektywniejszych narzędzi, służących do zabezpieczania wewnętrznych użytkowników sieci przed zagrożeniami zewnętrznymi. Zapora ogniowa stoi na granicy dwóch lub więcej sieci i kontroluje ruch pomiędzy nimi oraz pomaga zapobiec nieupoważnionemu dostępowi. Zapory ogniowe używają różnych technik w celu określenia, jaki dostęp do sieci ma zostać przepuszczony, a jaki zablokowany.

Ochrona systemów informatycznych określona w polityce bezpieczeństwa zakłada wykorzystywanie zapór ogniowych jako blokady przesyłania nieautoryzowanych danych między sieciami wewnętrzną i zewnętrzną. Podstawowe funkcje tych urządzeń to:

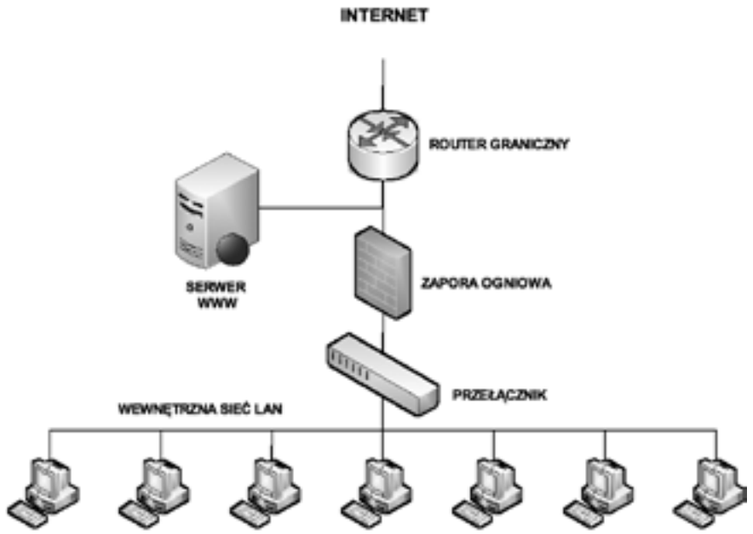
- ochrona adresów IP i przesyłanie komunikacji – dzięki tej funkcji możliwe jest tworzenie dodatkowych podsieci; mając do dyspozycji pojedynczy adres IP można utworzyć sieć lokalną LAN, a nawet rozległą WAN;
- oddzielenie sieci – zapora jest przede wszystkim narzędziem służącym do tworzenia granic między sieciami, nie musi ona jednak być umieszczona między siecią publiczną a prywatną; zapory ogniowe umieszcza się również wewnątrz sieci firmowych;
- ochrona przed atakami i skanowaniem – za pomocą zapór ogniowych można ograniczyć dowolny typ komunikacji sieciowej;
- filtrowanie adresów IP – funkcja ta umożliwia zarządzanie połączeniami w zależności od adresu IP oraz portu;
- filtrowanie zawartości – serwery pośredniczące proxy są jedynym typem zapór ogniowych, które są w stanie analizować komunikację badając adresy URL oraz zawartość stron WWW;
- przekierowywanie pakietów – funkcja ta polega na kierowaniu komunikacji na zupełnie inny port lub host niż ten, do którego został wysłany;
- uwierzytelnienie i szyfrowanie – zapora ogniowa umożliwia uwierzytelnienie użytkowników i szyfrowanie transmisji wykonywanych między nią a zaporą innej sieci;
- rejestrowanie komunikacji w dziennikach – zapora ogniowa umożliwia przegląd szczegółowych informacji na temat pakietów sieciowych przechodzących przez nią.

5.2 PRZYPADKI UŻYCIA ZAPORY OGNIOWEJ

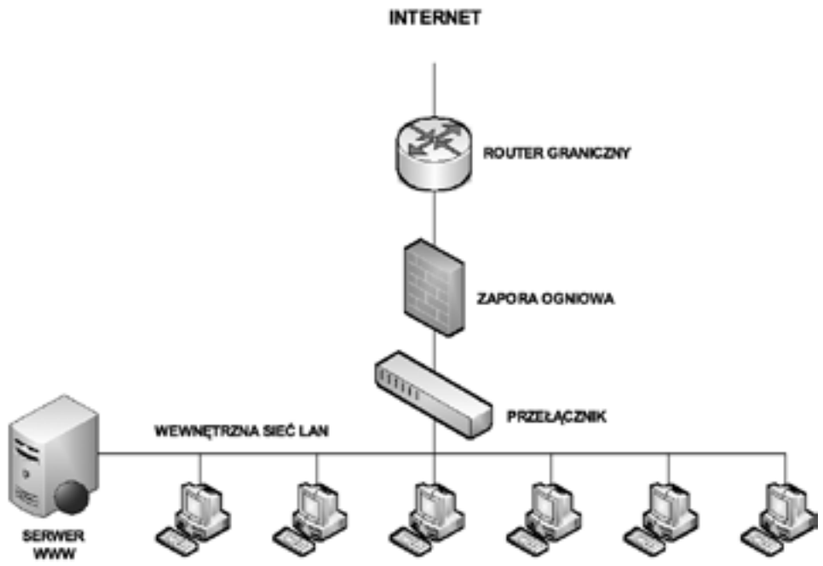
W sieci z rysunku 23 zastosowano zaporę ogniową do ochrony wewnętrznych zasobów sieci komputerowej. Natomiast serwer WWW dedykowany klientom z Internetu jest całkowicie dostępny na ataki, a jego działanie uzależnione jest od zastosowanej platformy serwerowej i poprawności konfiguracji.

W przypadku przedstawionym na rysunku 24, pomimo że serwer WWW jest umieszczony za zaporą ogniową, nie jest to rozwiązanie jeszcze idealne. Konfiguracja umożliwiająca przepuszczanie ruchu na porcie 80 (protokół http) i 443 (protokół https), niezbędna dla zapewnienia właściwej obsługi ruchu przychodzącego, daje włamywaczowi możliwość przeprowadzenia ataku na wewnętrzną sieć LAN.

Rysunek 25 przedstawia zastosowanie **strefy zdemilitaryzowanej** (ang. *Demilitarized Zone,* DMZ). Określenie to zostało zapożyczone z terminologii wojskowej, gdzie DMZ jest obszarem pomiędzy wrogimi siłami, w którym aktywność militarna jest zakazana. W sieciach komputerowych DMZ jest obszarem sieci, który jest dostępny zarówno dla wewnętrznych, jak i zewnętrznych użytkowników. Jest bardziej bezpieczny od zewnętrznej sieci, lecz mniej bezpieczny od wewnętrznej. Obszar ten jest tworzony przez jedną lub kilka zapór ogniowych i ma za zadanie odseparowanie sieci zewnętrznej i wewnętrznej od siebie. Serwery WWW przeznaczone do publicznego dostępu często umieszcza się właśnie w DMZ.



Rysunek 23.
Zapora ogniowa chroniąca wewnętrzną sieć LAN



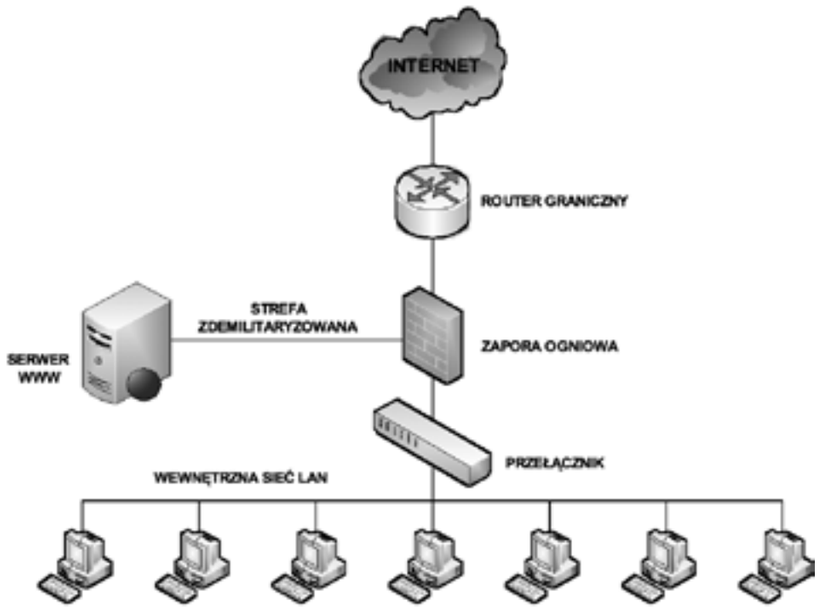
Rysunek 24.
Zapora ogniowa chroniąca wewnętrzną sieć LAN oraz serwer WWW

W wariancie z rysunku 26 zastosowano dwie zapory ogniowe ze strefą DMZ umieszczoną pomiędzy nimi. Zewnętrzna zapora ogniowa jest mniej restrykcyjna i zezwala użytkownikom z Internetu na dostęp do usług w DMZ, jednocześnie przepuszczając ruch zainicjowany przez użytkowników wewnętrznych. Wewnętrzna zapora ogniowa jest bardziej restrykcyjna – chroni wewnętrzną sieć przed nieupoważnionym dostępem.

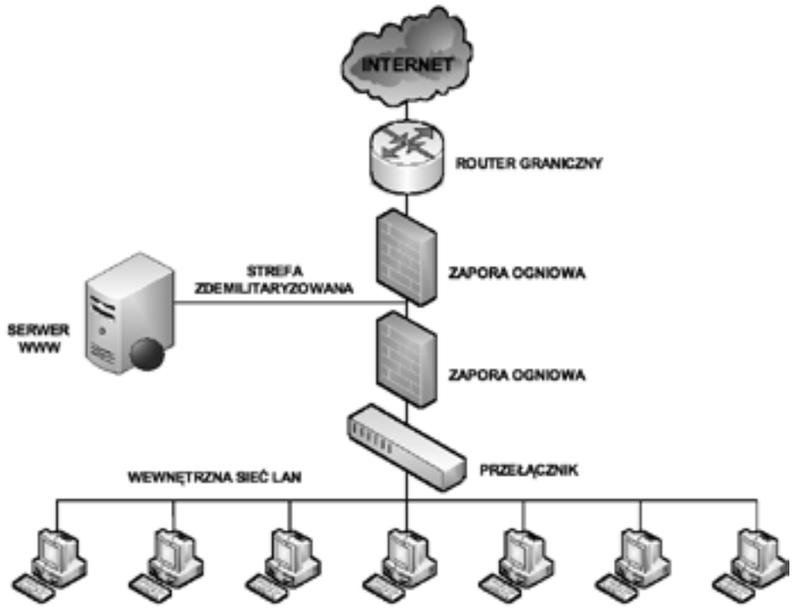
Konfiguracja z jedną zaporą ogniową jest zalecana w mniejszych sieciach. Taka konfiguracja stanowi pojedynczy punkt awarii i jednocześnie sama zapora może zostać przeciążona. Konfiguracja z dwiema zaporami ogniowymi jest polecana dla większych i bardziej rozbudowanych sieci, gdzie natężenie ruchu jest znacznie większe.

Planowanie bezpieczeństwa sieciowego wymaga oceny ryzyka związanego z utratą danych, uzyskaniem nieautoryzowanego dostępu. Plan musi również uwzględniać czynnik kosztów, stopień wyszkolenia personelu, platformy i sprzęt wykorzystywany w sieci.

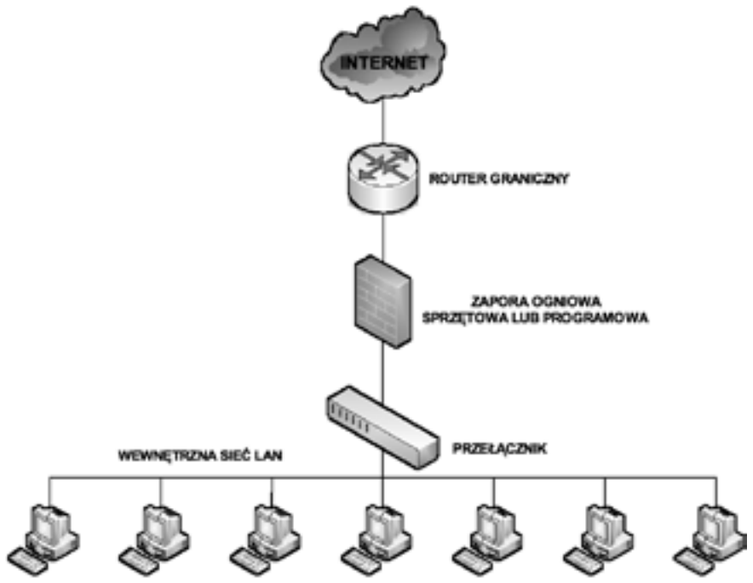
Zapory ogniowe, a co za tym idzie strefy DMZ, zapewniają wielowarstwowy model bezpieczeństwa. W przeszłości zapory ogniowe były wykorzystywane jedynie do podziału sieci na dwie części, sieć wewnętrzną i zewnętrzną (publiczną). Obecnie, ze względu na dostępność narzędzi służących włamaniom i łatwość z jaką mogą być przeprowadzane ataki, włącznie z atakami wykorzystującymi fałszowanie adresów, niezbędne jest dokładniejsze izolowanie sieci i lepsza ochrona przechowywanych w niej sieci. Służy temu stosowanie stref zdemilitaryzowanych.



Rysunek 25.
Zapora ogniowa oddzielająca wewnętrzną sieć LAN od strefy zdemilitaryzowanej



Rysunek 26.
Zastosowanie dwóch zapór ogniowych



Rysunek 27.
Przykład budowy prostej strefy DMZ

LITERATURA

1. Dye M.A., McDonald R., Rufi A.W., *Akademia sieci Cisco. CCNA Exploration. Semestr 1*, WN PWN, Warszawa 2008
2. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
3. Mucha M., *Sieci komputerowe. Budowa i działanie*, Helion, Gliwice 2003
4. Szmit M., Tomaszewski M., Lisiak D., Politowska I., *13 najpopularniejszych sieciowych ataków na Twój komputer. Wykrywanie, usuwanie skutków i zapobieganie*, Helion, Gliwice 2008
5. Szmit M., Gusta M., Tomaszewski M., *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion, Gliwice 2005