Zeszyty Naukowe WWSI, No 13, Vol. 9, 2015, s. 33-56

Wybrane zagadnienia bezpieczeństwa danych w sieciach komputerowych

Dariusz Chaładyniak*

Warszawska Wyższa Szkoła Informatyki

Streszczenie

Bezpieczeństwo danych przesyłanych w sieciach komputerowych jest jednym z najważniejszych zadań współczesnej teleinformatyki. W artykule przedstawiono podstawowe rodzaje złośliwego oprogramowania oraz przykładowe metody ataków na systemy i sieci teleinformatyczne. Przedstawiono również wybrane narzędzia i aplikacje do zabezpieczania wymiany danych. Wyjaśniono działanie systemów wykrywania włamań oraz zaprezentowano metody przeciwdziałania atakom sieciowym z wykorzystaniem zapór ogniowych.

Słowa kluczowe – złośliwe oprogramowanie, ataki sieciowe, systemy wykrywania włamań, zapory ogniowe

1 Złośliwe oprogramowanie

Złośliwe oprogramowanie (ang. *malicious software*) to programy, które mogą 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 mogą się same replikować i rozprzestrzeniać na inne hosty dołączone do sieci. Czasem techniki te są używane w połączeniu z socjotechniką, aby oszukać nieostrożnego użytkownika,

* E-mail: dchalad@wwsi.edu.pl

Zgłoszono do druku 30 października 2015 r.

by ten nieświadomie uruchomił taki atak. Poniżej przedstawiono wybrane przykłady złośliwego oprogramowania.

Wirus jest programem, który działa i rozprzestrzenia się przez modyfikowanie innych programów lub plików. Wirus nie może uruchomić się sam, musi zostać uaktywniony. 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.

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.

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.

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.

Spyware jest złośliwym oprogramowaniem mającym 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).

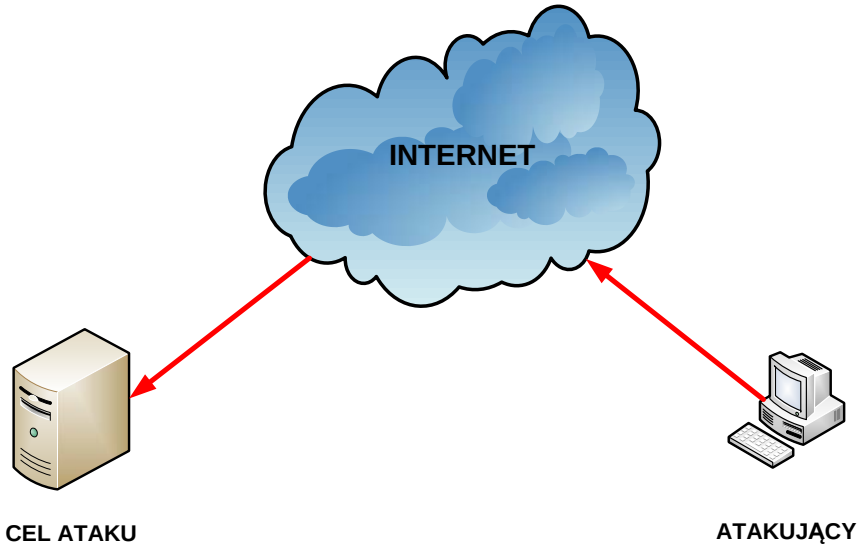
Stealware jest oprogramowaniem mającym na celu okradanie nieświadomego użytkownika poprzez śledzenie jego działań. Instalacja takiego programu odbywa się bez wiedzy i zgody użytkownika za pomocą odpowiednio spreparowanych wirusów komputerowych, robaków lub stron WWW wykorzystujących błędy i luki w przeglądarkach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

2 Wybrane ataki na sieci teleinformatyczne

2.1 Sposoby atakowania sieci

2.1.1 Atak zewnętrzny

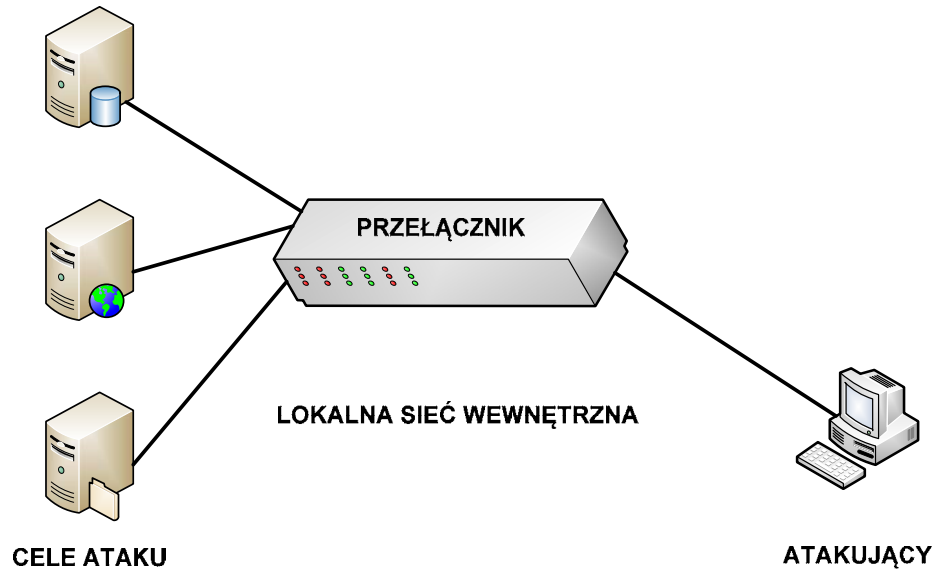
Ten sposób złośliwego oddziaływania (rysunek 1) jest powodowany przez osoby, które nie pracują w danej organizacji. Atakujący z zewnątrz toruje sobie drogę do sieci głównie przez Internet.



Rysunek 1. Przykład ataku z sieci zewnętrznej

2.1.2 Atak wewnętrzny

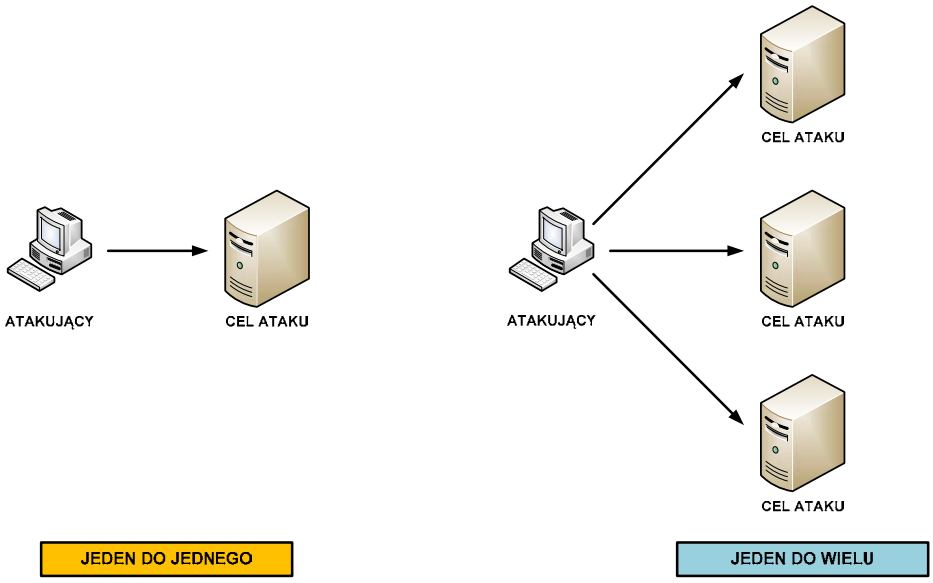
Taki rodzaj ataku (rysunek 2) może przeprowadzić ktoś, kto ma dostęp do sieci, czyli posiada konto lub ma dostęp fizyczny. Atakujący przeważnie zna ludzi oraz politykę wewnętrzną firmy. Nie wszystkie wewnętrzne ataki są celowe. W niektórych przypadkach zagrożenie wewnętrzne może powodować niefrasobliwy 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 większość zagrożeń pochodzi ze źródeł wewnętrznych. Jak podają statystyki, dostęp z wewnątrz i nadużycie systemów komputerowych stanowi ok. 70% zgłoszonych naruszeń bezpieczeństwa.



Rysunek 2. Przykład ataku z sieci wewnętrznej

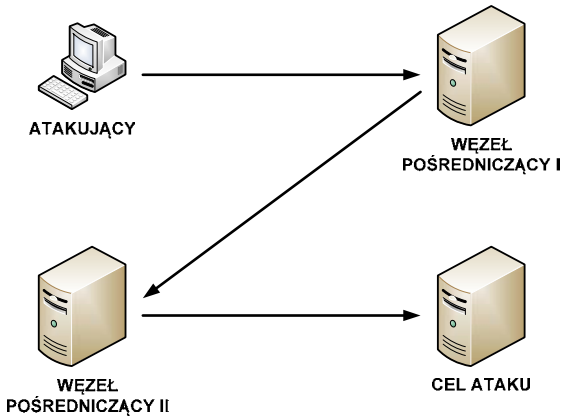
2.1.3 Atak tradycyjny

Ta forma (rysunek 3 – na następnej stronie) polega na atakowaniu z jednego komputera jednego lub wielu hostów sieciowych.



Rysunek 3. Przykłady ataków tradycyjnych

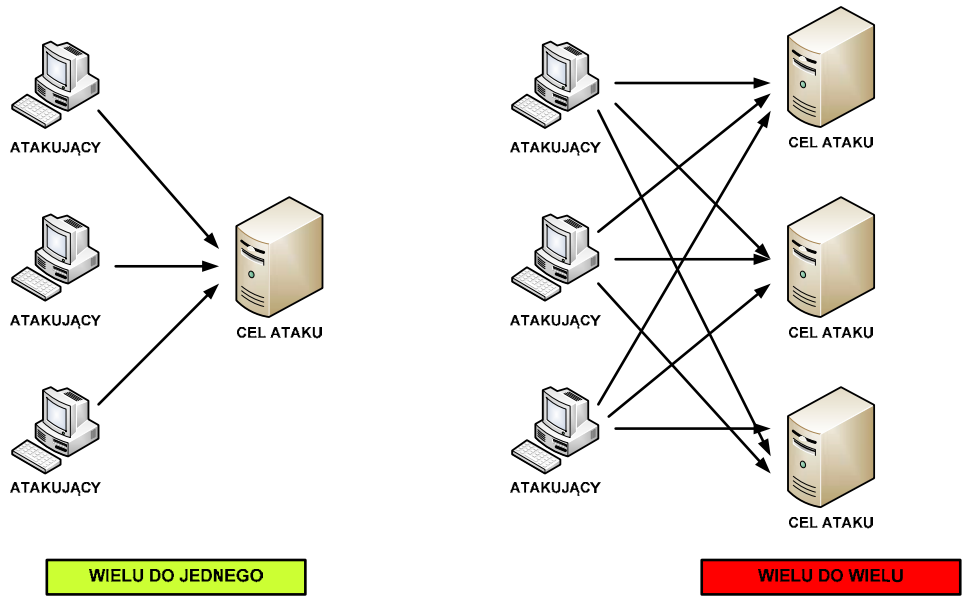
Często zdarza się, że włamywacze nie atakują bezpośrednio, a korzystają z komputerów ofiar dla ukrycia prawdziwego źródła ataku oraz utrudnienia ich odnalezienia. Jak widać na rysunku 4, intruz korzysta z kilku węzłów pośredniczących tak, aby atakowany obiekt zinterpretował je jako źródła ataków.



Rysunek 4. Przykład ataku przy udziale węzłów pośredniczących

2.1.4 Atak rozproszony

Zdarzenie takie (rysunek 5) 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.



Rysunek 5. Przykłady ataków rozproszonych

2.2 Rodzaje włamań sieciowych

Po uzyskaniu dostępu do sieci kraker (ang. *cracker*) może powodować następujące zagrożenia:

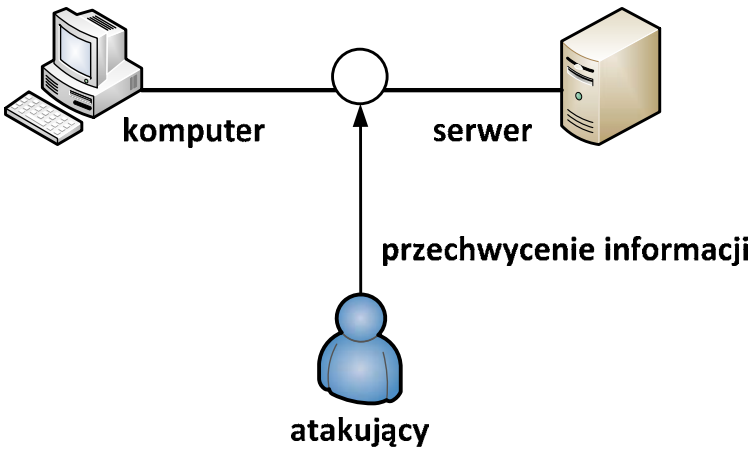
1. **Kradzież informacji** – włamanie do komputera w celu uzyskania poufnych informacji. Skradzione informacje mogą zostać użyte do różnych celów lub sprzedane.

2. **Kradzież tożsamości** – forma kradzieży, w której przedmiotem kradzieży stają się informacje osobiste, mająca na celu przejęcie czyjeś 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.

2.3 Rodzaje ataków sieciowych

2.3.1 Podsłuch sieciowy (ang. *sniffing*)

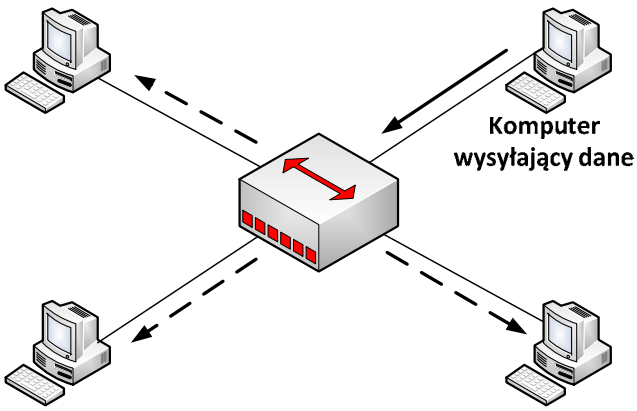
Podstawowym zagrożeniem, z którym każdy może się spotkać jest nieuprawnione przechwycenie (podsłuchanie) danych (rysunek 6). Może ono dotyczyć informacji zgromadzonych w komputerze, bądź informacji przesłanej poprzez sieć komputerową. Działanie atakującego polega na przechwytywaniu danych transmitowanych pomiędzy komputerem a serwerem. Taka analiza ruchu sieciowego umożliwia wychwycenie istotnych informacji np. loginów, haseł czy danych osobowych. Podsłuch jest najczęściej początkową fazą ataku i służy do zebrania niezbędnych informacji w celu dokonania późniejszego włamania do kolejnych komputerów lub serwerów w sieci.



Rysunek 6. Przykład podsłuchu sieciowego [1]

2.3.1.1 *Klasyczny sniffing pasywny*

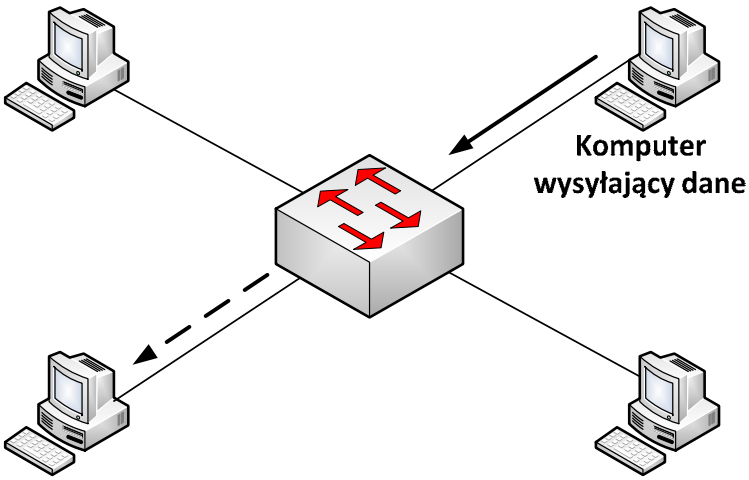
Dawno temu, kiedy sieci budowano przy użyciu kabla koncentrycznego, ewentualnie przy wykorzystaniu koncentratorów, każda wysłana informacja trafiała do wszystkich podłączonych do sieci komputerów. Każda ramka przesyłanej informacji opatrzona była adresem MAC karty sieciowej odbiorcy. Karty sieciowe w poszczególnych komputerach przetwarzały jedynie tę informację, która była zaadresowana do tej konkretnej karty. Do podsłuchania wystarczyło przedstawienie karty w tryb zwany **promiscuous**, który umożliwiał przechwytywanie informacji pochodzącej z całej sieci lokalnej. Działanie klasycznego sniffera w takiej sieci było działaniem pasywnym, to znaczy atakujący nie umieszczał dodatkowych informacji w sieci ani w podsłuchiwanym komputerze (rysunek 7).



Rysunek 7. Przykład podsłuchu pasywnego [1]

2.3.1.2 *Sniffing aktywny*

Karierę klasycznego sniffingu przerwało upowszechnienie przełączników sieciowych, które rozpoznają adresy MAC odbiorcy i przełączają informację tylko na ten ze swoich portów, do którego fizycznie dołączony jest komputer o żądanym adresie. Do podsłuchu w sieciach przełączanych należało posłużyć się znacznie bardziej skomplikowanymi metodami jak **ARP spoofing** czy **MAC flooding** (zalewanie przełącznika dużą ilością ramek ze sfałszowanym adresem MAC w celu przepełnienia pamięci urządzenia), które są atakami aktywnymi, a co za tym idzie, znacznie łatwiejszymi do wykrycia (rysunek 8).



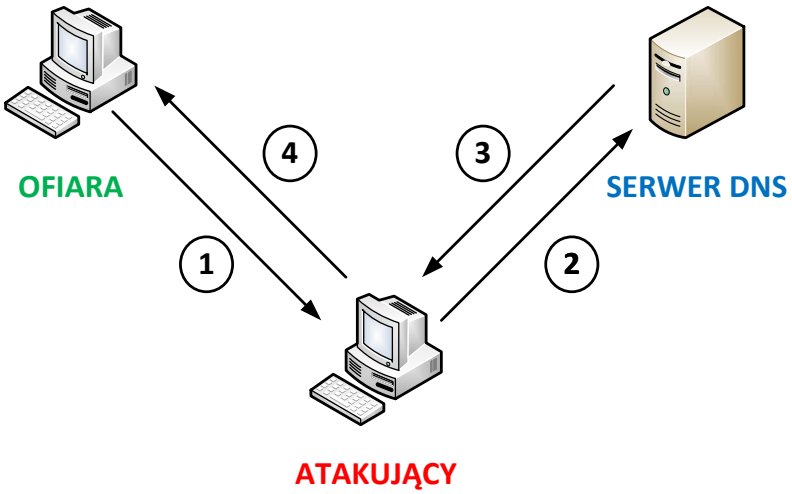
Rys. 2.8. Przykład podsłuchu aktywnego [1]

2.3.2 ARP spoofing

ARP spoofing polega na wysyłaniu sfałszowanego pakietu ARP Reply, na podstawie którego komputery w sieci są informowane o odwzorowaniach adresów logicznych IP na adresy fizyczne MAC. Nadawca wysyła zapytanie o konkretny adres IP. Odpowiedź na to zapytanie wysyła komputer atakującego, podając swój adres MAC. W komputerze wysyłającego dokonywany jest wpis w dynamicznej tablicy ARP – odwzorowanie szukanego adresu IP na adres MAC komputera atakującego. W ten sposób komunikacja zamiast z rzeczywistym odbiorcą odbywa się z komputerem atakującego. Dodatkowo komputer atakującego wysyła zapytanie o adres IP rzeczywistego odbiorcy i po jego odpowiedzi może przekazywać mu informacje. W ten sposób komunikacja jest niezauważona, a atakujący ma możliwość przeglądania i modyfikowania przesyłanych danych.

2.3.3 DNS spoofing

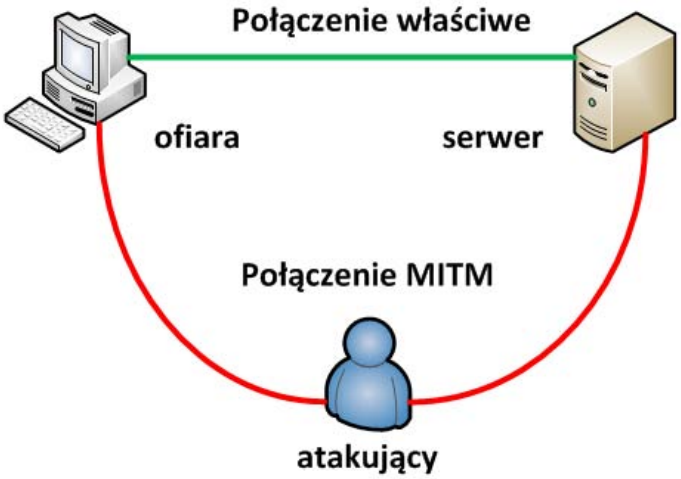
Atak DNS spoofing polega na uruchomieniu fałszywego serwera nazw domenowych (DNS) nasłuchującego na porcie 53 (rys. 2.9). Do serwera tego kierowane są zapytania DNS przechwycone przez atakującego (np. z użyciem techniki ARP spoofing). Zwracane przez serwer fałszywe odwzorowania nazw domenowych na adresy IP umożliwiają przekierowanie ruchu na nieprawidłowy serwer. Inną metodą znacznie trudniejszą, jest włamanie się do serwera DNS i podmiana tablicy odwzorowań nazw.



Rysunek 9. Przykład ataku DNS spoofing [1]

2.3.4 Man in the Middle

Man in the middle – „**człowiek pośrodku**" – to radzaj ataku polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy (rysunek 10).



Rysunek 10. Przykład ataku Man in the Middle [1]

2.3.5 Atak słownikowy i brute force

Atak słownikowy to technika używana do łamania haseł w swoim działaniu zbliżona do metody brute force. Główna różnica między tymi metodami polega na sposobie dobierania haseł, które należy przetestować.

Brute force wybiera kolejne znaki i sprawdza ich wszystkie możliwe kombinacje w celu odnalezienia właściwego wzoru.

Atak słownikowy korzysta z wyrażeń bazujących na zawartości słownika, co znacznie zmniejsza liczbę testowanych kombinacji, jednak zmniejsza prawdopodobieństwo odniesienia sukcesu.

2.3.6 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, jak ostatnio, przez komunikatory sieciowe.

2.3.7 Atak DoS

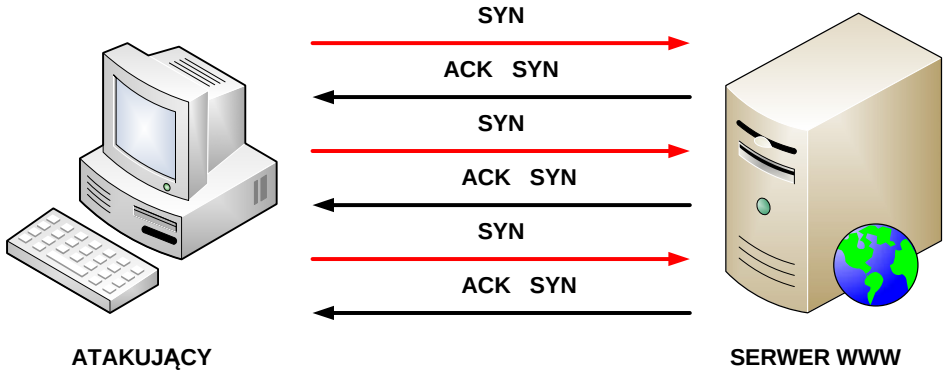
Ataki DoS (ang. *Denial of Service*) są prowadzone na pojedyncze komputery lub grupy komputerów i mają na celu uniemożliwienie korzystania z usług. Celem ataku DoS mogą być systemy operacyjne, serwery, routery i łącza sieciowe. Główne cele ataków DoS to:

1. Zalanie systemu (lub sieci) ruchem, aby zablokować ruch pochodzący od użytkowników.
2. 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 (rysunek 11).
2. **Ping śmierci** (ang. *Ping of death*) – do urządzenia sieciowego wysyłany jest pakiet o rozmiarze większym niż maksymalny (65535 bajtów). Taki pakiet może spowodować awarię systemu.

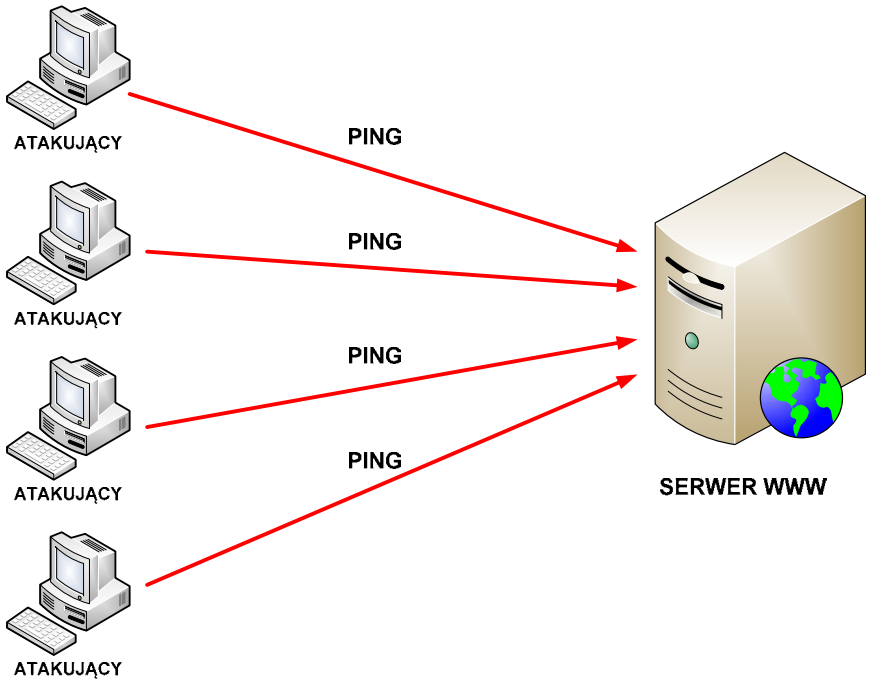


Rysunek 11. Przykład ataku typu DoS

2.3.8 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 (rysunek 12).



Rysunek 12. Przykład ataku typu DDoS

2.3.9 DNS Amplification

DNS Amplification to odmiana ataku DDoS, polegająca na wysłaniu zapytań do serwerów DNS ze sfałszowanym adresem zwrotnym (*spoofing*). Najczęściej wykorzystuje się do tego sieć przejętych przez agresora komputerów (*botnet*). Serwery DNS, w odpowiedzi na dziesiątki lub nawet setki tysięcy zapytań kierowanych z komputerów agresora, wysyłają odpowiedzi na jeden komputer, cel ataku włamywacza, zapychając jego łącze, pamięć i moc obliczeniową. Atakowany ma małe możliwości obrony przed takim atakiem, gdyż odfiltrowanie odpowiedzi od DNS na odpowiedzi na zadane i na niezadane pytanie jest praktycznie niemożliwe. W maju 2006 w ten właśnie sposób zostało zaatakowane i doprowadzone do upadku przedsiębiorstwo Blue Security, które walczyło ze spamem.

2.3.10 IP spoofing

IP Spoofing to termin określający fałszowanie źródłowego adresu IP w wysyłanym przez komputer pakiecie sieciowym. Taki atak może służyć ukryciu tożsamości atakującego (np. w przypadku ataków DoS), podszyciu się pod innego użytkownika

sieci i ingerowanie w jego aktywność sieciową, lub wykorzystaniu uprawnień posiadanych przez inny adres (atak wykorzystany przez Kevina Mitnicka w celu dostania się do komputera Tsutomu Shimomury). Obecnie ataki tego typu są w pewnym stopniu udaremniane przez filtrowanie wprowadzone przez niektórych dostawców usług internetowych, a także stosowanie kryptograficznych zabezpieczeń komunikacji i trudnych do odgadnięcia początkowych numerów sekwencyjnych TCP/IP.

2.3.11 Ping flood

Ping flood to popularny sposób ataku na serwer internetowy polegający na przeciążeniu łącza pakietami ICMP generowanymi na przez program ping. Przeprowadza się go za pomocą komputera posiadającego łącze o przepustowości większej niż przepustowość łącza atakowanej maszyny, lub za pomocą wielu niezależnych komputerów. Atakowany serwer otrzymuje bardzo dużą ilość zapytań *ping* (*ICMP Echo Request*), odpowiadając na każde za pomocą (*ICMP Echo Reply*), co może doprowadzić do przeciążenia jego łącza i w konsekwencji niedostępności oferowanych serwisów. Jednym ze sposobów obrony przed tego typu atakiem jest firewall, który filtruje pakiety *ICMP Echo Request*.

2.3.12 Smurf attack

Smurf Attack (*atak smerfów*) jest potomkiem ataku sieciowego o nazwie ping flood, który polega na przeciążeniu łącza atakowanego systemu pakietami ping. W wypadku ataku ping flood intruz wykorzystuje swoją przewagę w przepustowości używanego łącza, natomiast Smurf Attack umożliwia skuteczną akcję użytkownikom łącza o słabszych parametrach niż to atakowanego systemu. Atak ten polega na technice fałszowania zapytań ping (*ICMP Echo Request*), poprzez zamianę adresu źródła tych zapytań na adres atakowanego serwera. Tak spreparowane pakiety ping, wysyłane są na adres rozgłoszeniowy sieci zawierającej wiele komputerów. Pakiety zostają rozesłane do wszystkich aktywnych systemów w sieci, co powoduje przesłanie przez nie pakietów *ICMP Echo Reply* na sfałszowany wcześniej adres źródłowy atakowanej ofiary.

2.3.13 SYN flood

SYN flood to jeden z popularnych ataków w sieciach komputerowych. Jego celem jest głównie zablokowanie usług danego serwera (DoS). Do przeprowadzenia ataku wykorzystywany jest protokół TCP. Atak polega na wysyłaniu dużej ilości pakietów z ustawioną w nagłówku flagą synchronizacji (SYN) i ze sfałszowanym adresem IP nadawcy (*IP spoofing*). Pakiety TCP z ustawioną flagą SYN służą do informowania zdalnego komputera o chęci nawiązania z nim połączenia. Podczas takiego ataku

serwer, który otrzymał pakiet z flagą SYN na port, który jest otwarty odpowiada na każdy pakiet zgodnie z zasadami protokołu TCP wysyłając pakiet z ustawionymi flagami synchronizacji (SYN) i potwierdzenia (ACK) do komputera, który w tym wypadku:

- nie istnieje;
- istnieje, ale nie zamierzał nawiązywać połączenia z atakowanym hostem;
- jest to komputer atakowanego, który specjalnie nie odpowiada.

Powoduje to przesyłanie dużych ilość danych i obciąża łącze sieciowe.

2.3.14 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.

2.4 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 mogą zawierać złożone implementacje zapór ogniowych i systemów wykrywania włamań.

Przykłady narzędzi i aplikacji używanych do zabezpieczania sieci:

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.

3 Systemy wykrywania intruzów (włamań)

3.1 Systemy IDS

Zadaniem **systemu wykrywania intruzów** (IDS – ang. *Intrusion Detection System*) 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.

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:

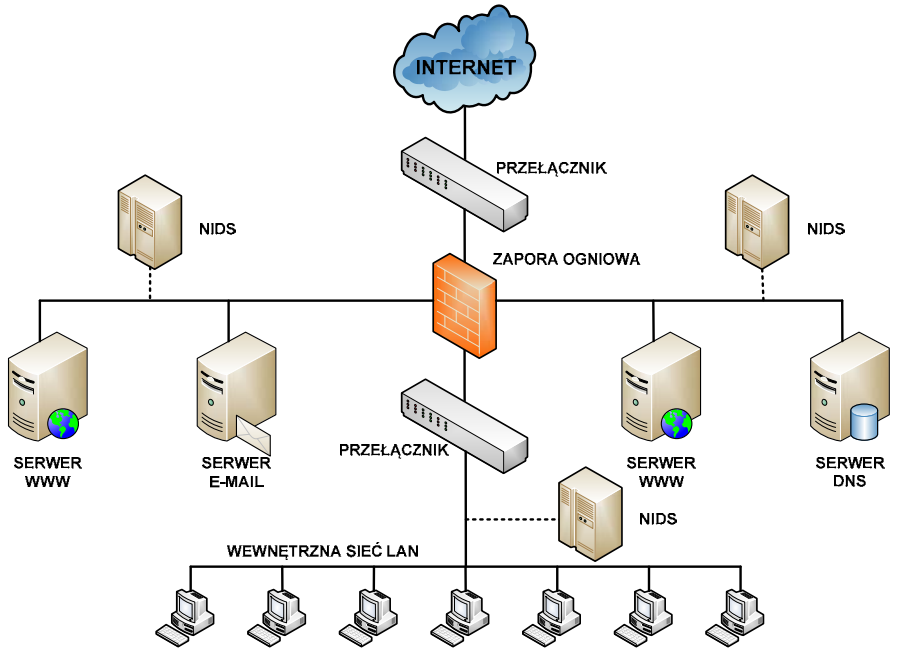
1. **Dopasowywanie wzorców** – jest to najprostsza metoda detekcji intruza; pojedynczy pakiety porównywany jest z listą reguł. Jeśli któryś z warunków jest spełniony, to jest uruchamiany alarm.
2. **Kontekstowe dopasowywanie wzorców** – w kontekstowym dopasowywaniu pakietu, system bierze pod uwagę kontekst każdego pakietu. Śledzi połączenia, dokonuje łączenia fragmentowanych pakietów.
3. **Analiza heurystyczna** – wykorzystuje algorytmy do identyfikacji niepożądanego działania. Są one 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 odbiegający od normy ruch sieciowy. Największym problemem jest określenie stanu uważanego za normalny.

3.2. Rodzaje systemów IDS

Wyróżnia się trzy główne rodzaje systemów IDS:

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

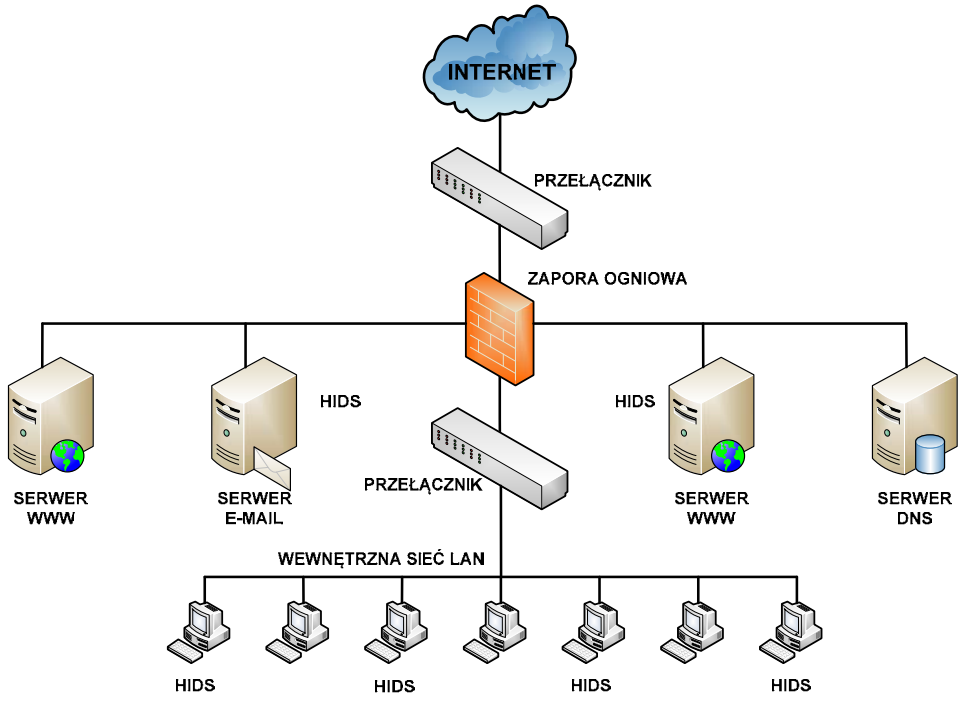
Na rysunku 3.1 pokazano schemat sieciowego systemu wykrywania intruzów (NIDS). Takie rozwiązanie umożliwia skuteczne monitorowanie wydzielonego segmentu sieci. System NIDS może podsłuchiwać wszelką komunikację prowadzoną w tej sieci. To rozwiązanie jest nastawione na ochronę publicznie dostępnych serwerów zlokalizowanych w podsieciach stref zdemilitaryzowanych.



Rysunek 13. Schemat systemu wykrywania włamań typu NIDS [2]

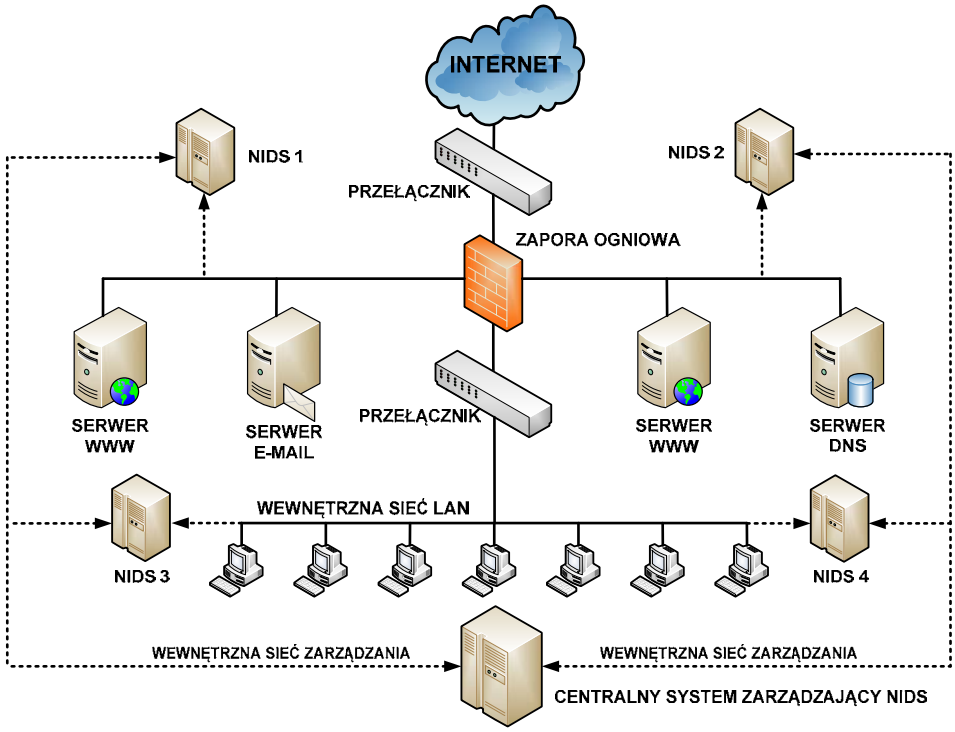
Schemat hostowego systemu wykrywania intruzów (HIDS) jest przedstawiony na rysunku 13. Podstawowa różnica między systemami HIDS a NIDS polega na tym,

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 14. Schemat systemu wykrywania włamań typu HIDS [2]

Na rysunku 14 pokazano 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. Zgodnie z przedstawionym schematem, sensory NIDS1 i NIDS2 operują w cichym trybie odbierania i chronią serwery dostępu publicznego. Z kolei sensory NIDS3 i NIDS4 chronią systemy hostów znajdujących się wewnątrz sieci zaufanej.



Rysunek 15. Schemat systemu wykrywania włamań typu NNIDS [2]

4 Działanie zapór ogniowych

4.1 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.

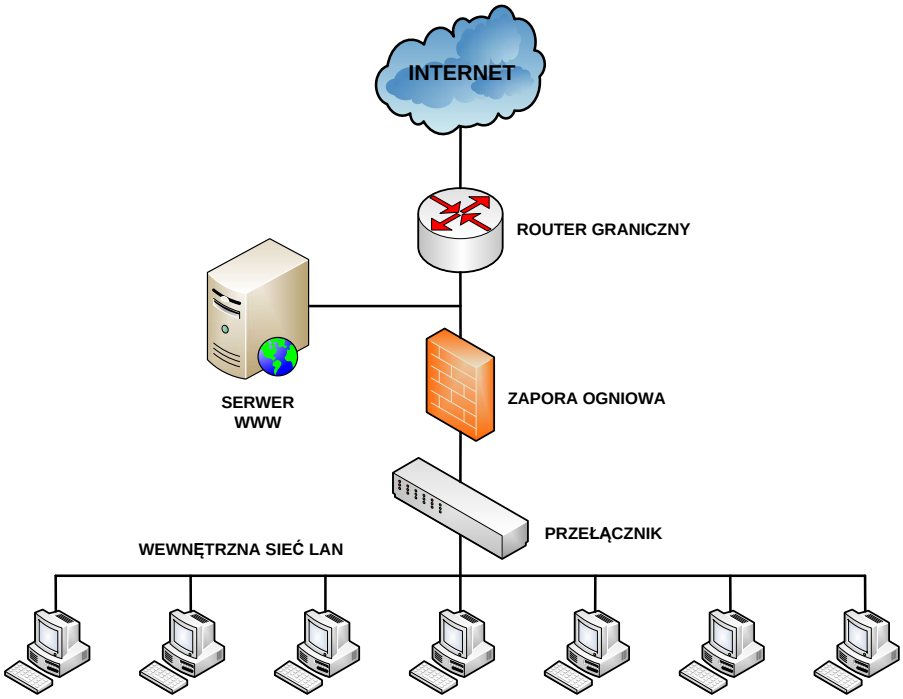
Podstawowe funkcje tych urządzeń to:

- ochrona adresów IP i przesyłanie komunikacji,

- ochrona przed atakami i skanowaniem,
- filtrowanie adresów IP,
- filtrowanie zawartości,
- przekierowywanie pakietów,
- uwierzytelnienie i szyfrowanie,
- rejestrowanie komunikacji w dziennikach.

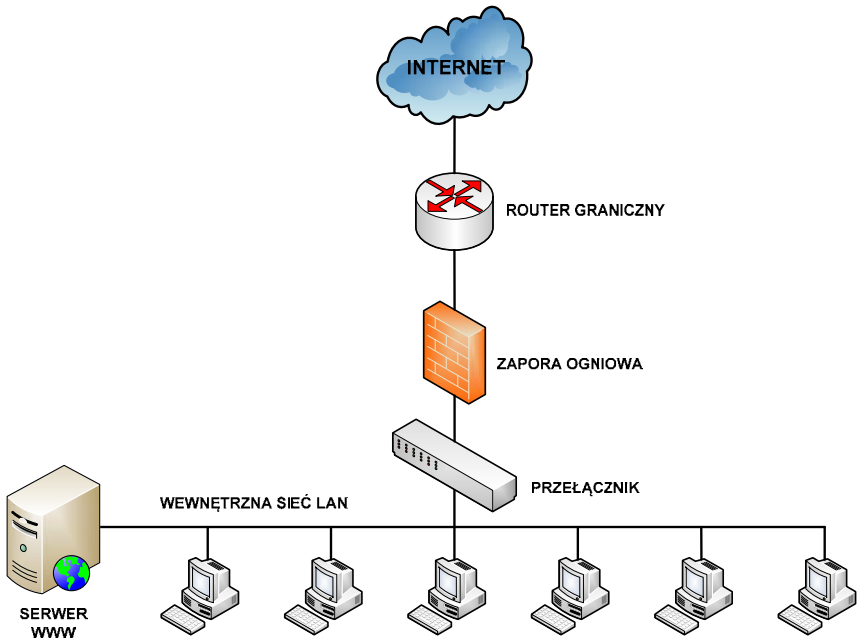
4.2. Przypadki użycia zapory ogniowej

W sieci z rysunku 16 zastosowano zaporę ogniową do ochrony wewnętrznych zasobów sieci komputerowej. Natomiast serwer WWW dedykowany dla klientów z Internetu jest całkowicie dostępny na ataki, a jego działanie uzależnione jest od zastosowanej platformy serwerowej i poprawności konfiguracji.



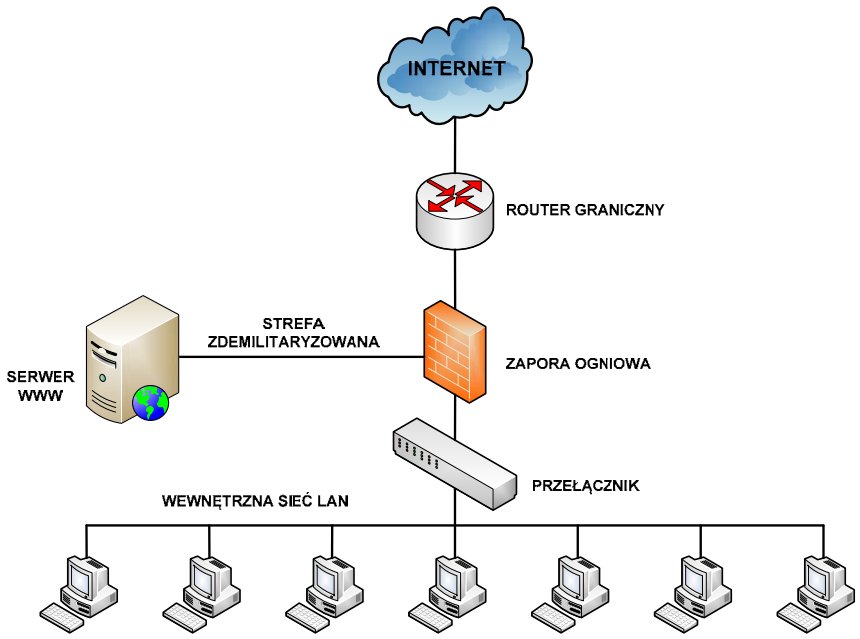
Rysunek 16. Zapora ogniowa chroniąca wewnętrzną sieć LAN [2]

W przypadku przedstawionym na rysunku 17, 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 17. Zapora ogniowa chroniąca wewnętrzną sieć LAN oraz serwer WWW [2]

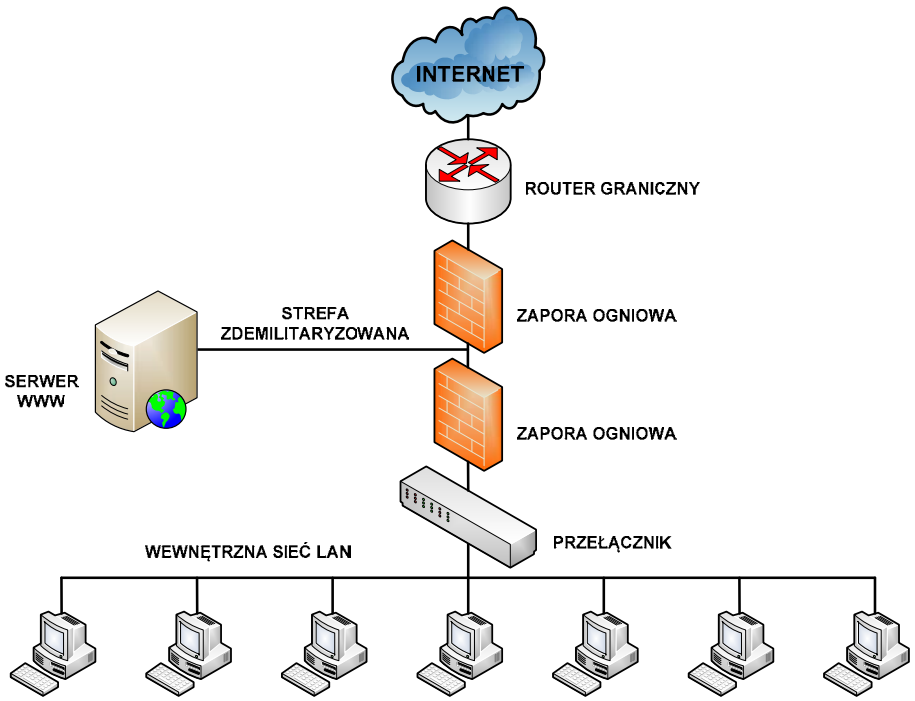
Na rysunku 18 (na następnej stronie) przedstawiono zastosowanie **strefy zdemilitaryzowanej** (ang. *Demilitarized Zone, DMZ*). W sieciach komputerowych, DMZ jest obszarem sieci, który jest dostępny zarówno dla wewnętrznych jak i zewnętrznych użytkowników. Jest bardziej bezpieczny od zewnętrznej sieci, 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 18. Zapora ogniowa oddzielająca wewnętrzną sieć LAN od strefy zdemilitaryzowanej [2]

W wariancie z rysunku 19 (na następnej stronie) 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.



Rysunek 19. Zastosowanie dwóch zapór ogniowych [2]

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.

Podsumowanie

W artykule przedstawiono wybrane zagadnienia związane z bezpieczeństwem i ochroną danych w sieciach teleinformatycznych. Ostatnie lata związane z ogromnym wzrostem ilości naruszeń bezpieczeństwa pokazały, że należy podjąć wszelkie działania zapobiegawcze w celu zahamowania rozwijającej się przestępczości internetowej. W obecnych czasach, gdy Internet jest coraz bardziej powszechny i coraz więcej ludzi korzysta z jego zasobów, bezpieczeństwo staje się priorytetem, które trzeba nieustannie udoskonalać. Zastosowanie zapór ogniowych, systemów IDS

i IPS, wdrożenie odpowiednich zasad bezpieczeństwa, uświadomienie użytkowników sieci a także ciągłe pogłębianie wiedzy w tym zakresie mogą znacznie przyczynić się do wzrostu bezpieczeństwa danych.

Bibliografia

[1] Szmit M., Tomaszewski M., Lisiak D., Politowska I., *13 najpopularniejszych sieciowych ataków na Twój komputer. Wykrywanie, usuwanie skutków i zapobieganie*, Helion, Gliwice 2008

[2] Szmit M., Gusta M., Tomaszewski M., *101 zabezpieczeń przed atakami w sieci komputerowej*, Helion, Gliwice 2005

Selected issues of data security in computer networks

Abstract

Security of data transmitted over computer networks is one of the most important tasks of modern ICT. The article presents basic types of malicious software and hacking attacks on ICT systems. It also presents some of the tools and applications for securing data exchange. Operation of intrusion detection systems and counter-attack methods using firewalls are presented.

Keywords – Malicious Software, network attacks, Intrusion Detection Systems, firewalls