Bezpieczeństwo sieci

Maciej Dawid

Złośliwe oprogramowanie

Złośliwe oprogramowanie (ang. malicious software) to programy, które muszą zostać wprowadzone na komputer 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 mogą same się replikować i rozprzestrzeniać na inne hosty dołączone do sieci. Czasem techniki te używane są w połączeniu z socjotechniką, aby oszukać nieostrożnego użytkownika, by ten nieświadomie uruchomił taki atak.

Wirusy

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 wirus może nie robić nic poza replikacją i rozprzestrzenianiem się.

Nawet nieskomplikowany typ wirusa jest niebezpieczny, gdyż może szybko zużyć całą dostępną pamięć i doprowadzić system do zatrzymania. Bardziej poważny wirus przed rozprzestrzenieniem może usunąć lub uszkodzić pliki. Wirusy mogą być przenoszone przez załączniki e-mail, pobierane pliki, komunikatory czy wreszcie przez dyskietki, płyty CD/DVD lub urządzenia USB.

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

Robak

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, My Doom, Netsky.

Koń trojański

Koń trojański (ang. trojan horse) 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 zwykle jest stosunkowo nieszkodliwy, ale może również zupełnie zniszczyć zawartość dysku twardego. Trojany często tworzą furtkę pozwalającą hakerom na pełny dostęp do zasobów komputera.

Najbardziej znane trojany to: Connect4, Flatley Trojan, Poison Ivy.

Inne zagrożenia

Bomby logiczne (ang. logical bombs) w odróżnieniu od konia trojańskiego nie uruchamiają ukrytego złośliwego oprogramowania od razu tylko w odpowiednim czasie (zajścia określonego zdarzenia lub kilkukrotnego uruchomienia danej 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.

Inne zagrożenia

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 ażeby odzyskał dane.

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

Inne zagrożenia

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). Najbardziej znane spyware to: Gator, Cydoor, Save Now.

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.

Rodzaje programów antywirusowych

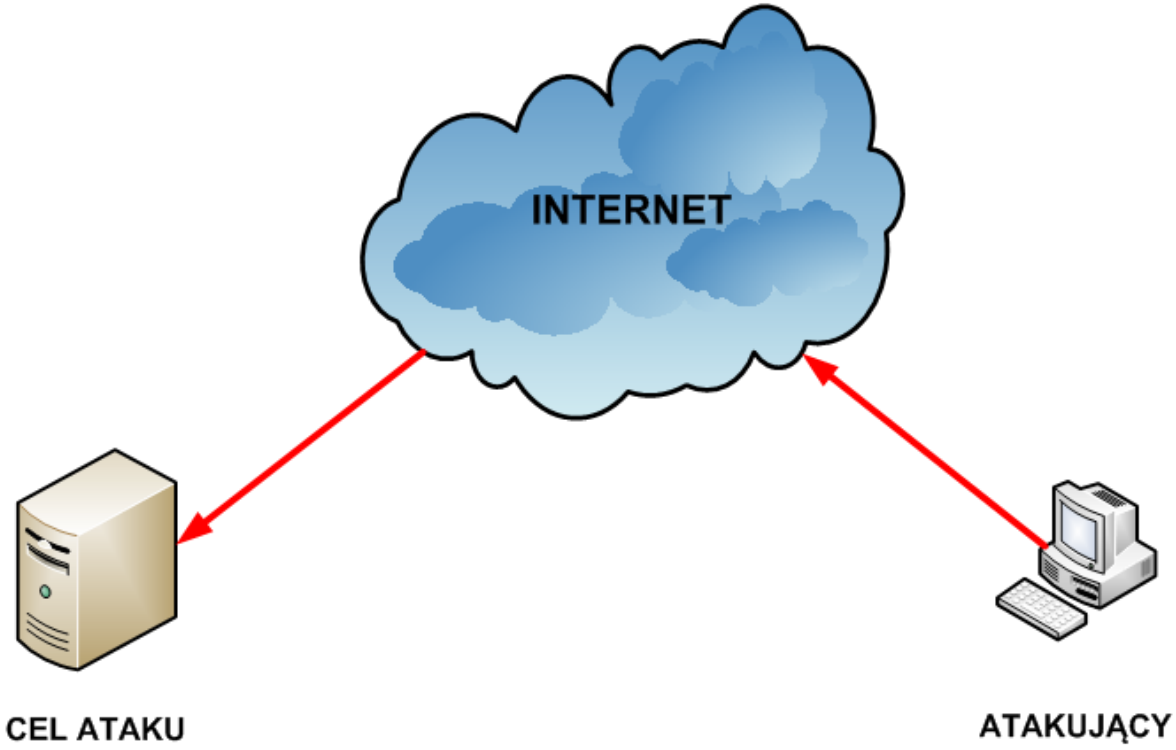
Skanery (ang. scaners) należą do najstarszych i najprostszych sposobów ochrony przed wirusami komputerowymi. Podstawowa zasada działania skanerów polega na wyszukiwaniu pewnej sekwencji bajtów w zadanym ciągu danych. Skaner jest tym skuteczniejszy im wirus zawiera w sobie bardziej charakterystyczny napis lub ciąg bajtów.

Monitory (ang. resident monitors) to oprogramowanie antywirusowe zainstalowane w systemie operacyjnym jako programy rezydentne. Skuteczność monitorów zależy od tego czy przejęły one kontrolę nad systemem przed działaniem wirusa czy po jego działaniu oraz od tego jak głęboko wnika on w system operacyjny.

Rodzaje programów antywirusowych

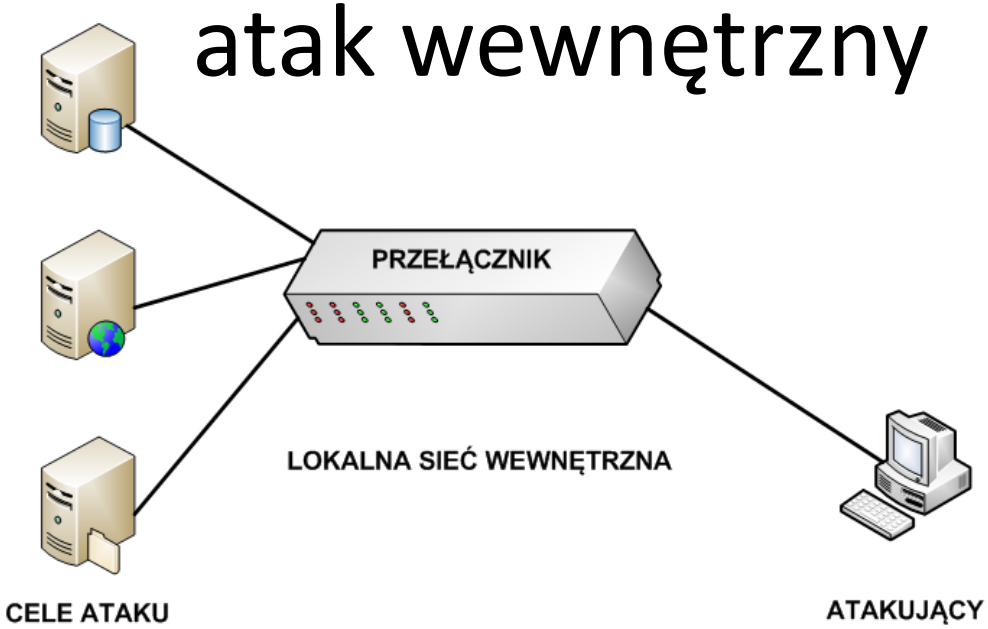
- **Szczepionki** (ang. disinfectors) są oprogramowaniem antywirusowym działającym przeciwko konkretnym infekcjom. Po wykryciu wirusa i poddaniu odpowiedniej analizie jego kodu można zdefiniować pewne właściwości pozwalające przygotować właściwą szczepionkę.
- **Programy zliczające sumy kontrolne** (ang. integrity checkers) przy pierwszym uruchomieniu dokonują odpowiednich obliczeń dla plików zgromadzonych na dysku a następnie wykorzystują te dane aby porównać z bieżąco wyliczoną sumą kontrolną i na tej podstawie stwierdzić ewentualną obecność wirusa.

Ataki na sieci teleinformatyczne – atak zewnętrzny



Ataki zewnętrzne powodowane są przez osoby, które nie pracują w danej organizacji. Atakujący z zewnątrz toruje sobie drogę do sieci głównie przez Internet, łącza bezprzewodowe lub usługi wdzwaniane.

Ataki na sieci teleinformatyczne – atak wewnętrzny

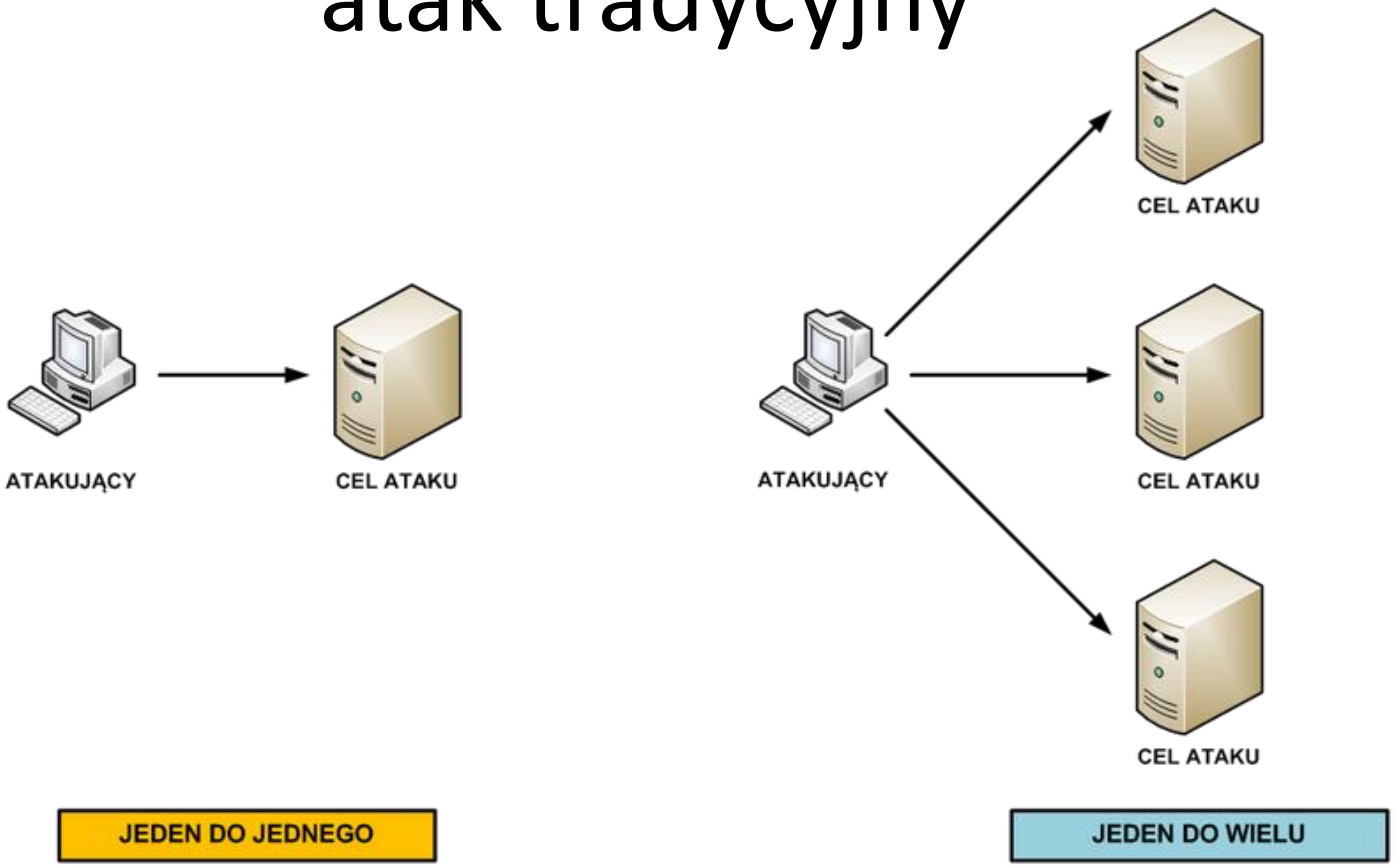


Atak wewnętrzny może przeprowadzić ktoś, kto posiada dostęp do sieci, czyli posiada konto lub ma dostęp fizyczny. Atakujący przeważnie zna ludzi oraz politykę wewnętrzną firmy.

Jednakże nie wszystkie wewnętrzne ataki są celowe. W niektórych przypadkach zagrożenie wewnętrzne powodować może niefrasobliwy pracownik, który ściągnie i uruchomi wirusa, a następnie nieświadomie wprowadzi go do wnętrza sieci.

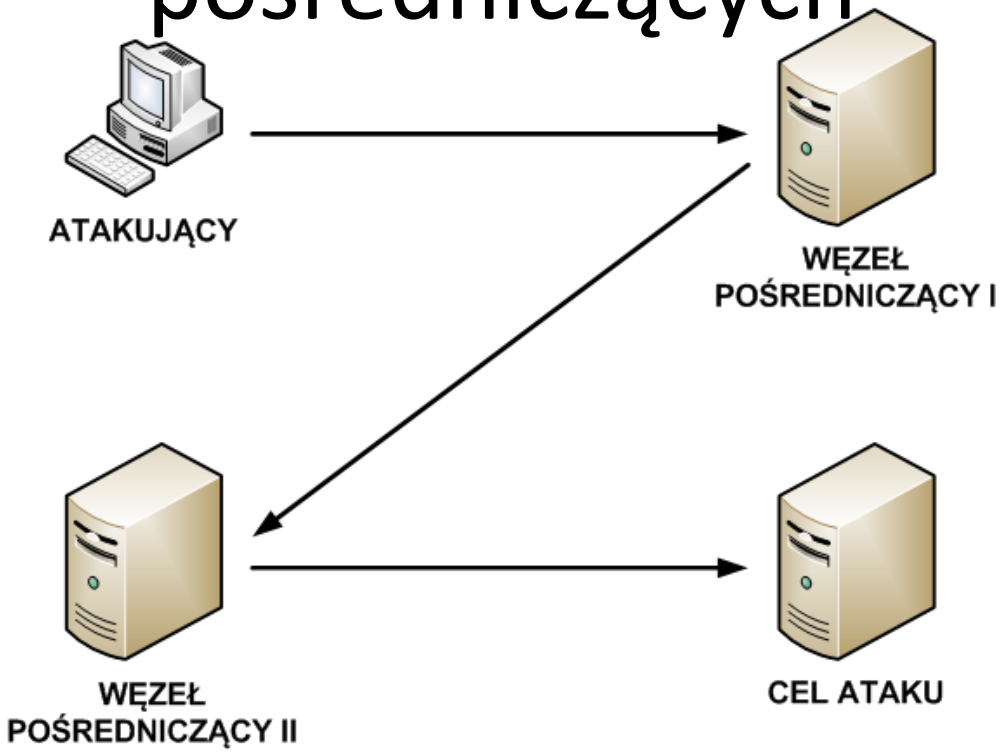
Większość firm wydaje znaczące sumy na ochronę przed zewnętrznymi atakami, mimo iż większość zagrożeń pochodzi ze źródeł wewnętrznych. Jak podają statystyki, dostęp z wewnątrz i nadużycie systemów komputerowych stanowi ok. 70% zgłoszonych naruszeń bezpieczeństwa.

Ataki na sieci teleinformatyczne – atak tradycyjny



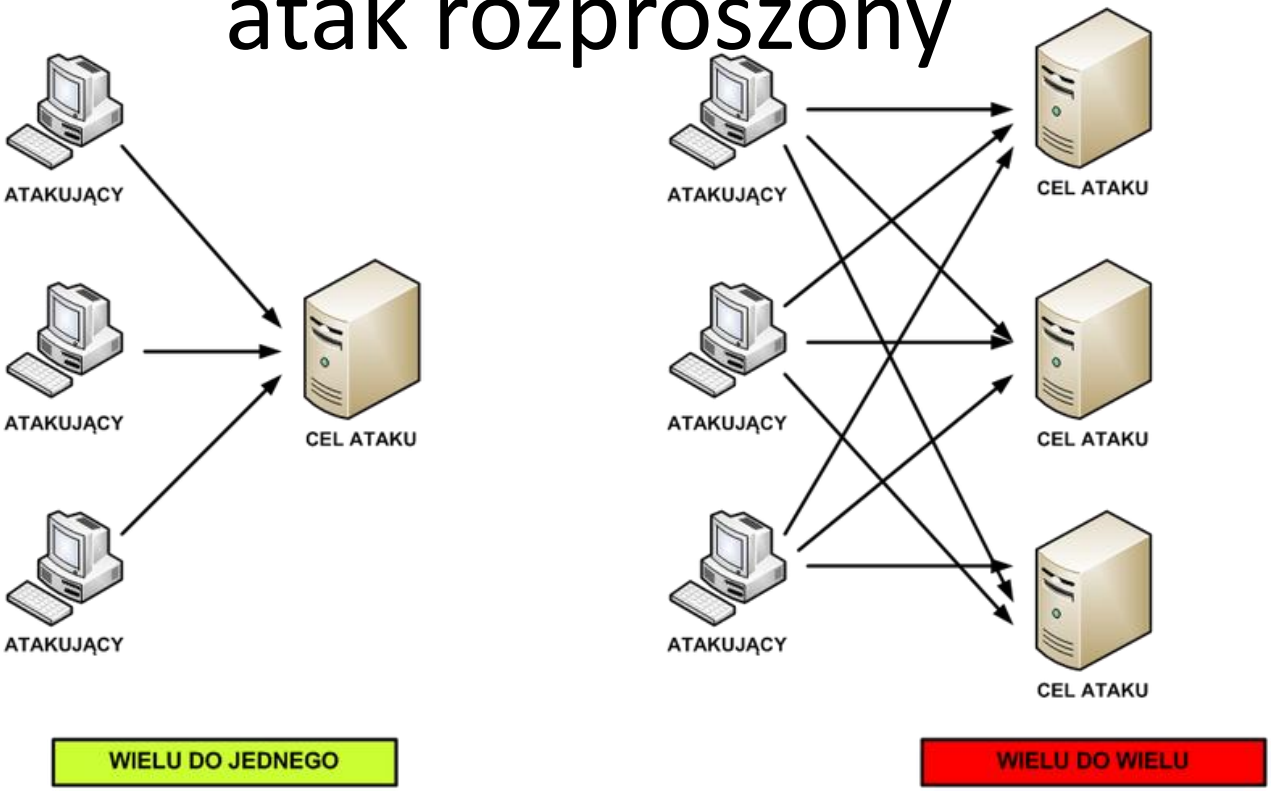
Atak tradycyjny polega na atakowaniu z jednego komputera jednego lub wielu hostów sieciowych.

Ataki na sieci teleinformatyczne – atak przy pomocy węzłów pośredniczących



Często zdarza się, że włamywacze nie atakują bezpośrednio. Korzystają oni z komputerów ofiar, w celu ukrycia prawdziwego źródła ataku oraz utrudnienia ich odnalezienia. Jak widać, intruz korzysta z kilku węzłów pośredniczących, tak aby atakowany obiekt zinterpretował je jako źródła ataków.

Ataki na sieci teleinformatyczne – atak rozproszony



Atak rozproszony 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 ataku rozproszonego jest fakt, iż pakiety atakującego nie są wysyłane z hosta atakującego ale z węzłów pośredniczących. 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.

Rodzaje włamań sieciowych

Kradzież informacji

Utrata i zmiana danych

Kradzież tożsamości

Blokada usług

Po uzyskaniu dostępu do sieci haker może powodować następujące zagrożenia:

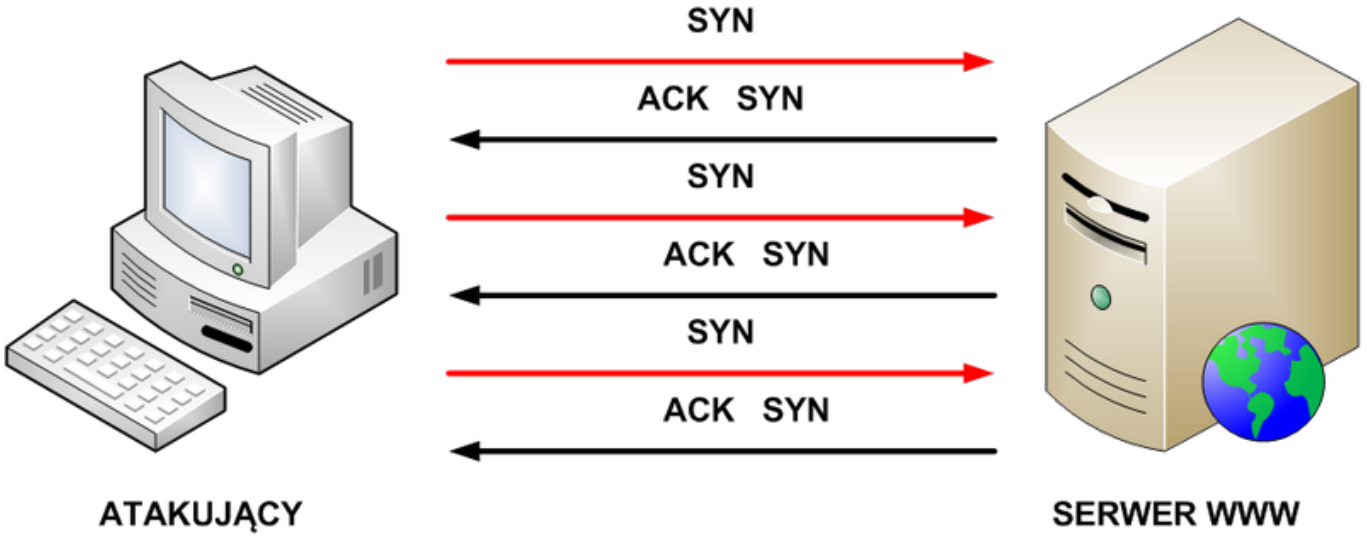
1. **Kradzież informacji** – włamanie do komputera celem uzyskania poufnych informacji. Skradzione informacje mogą zostać użyte do różnych celów lub sprzedane.
2. **Kradzież tożsamości** – forma kradzieży, w której przedmiotem kradzieży stają się informacje osobiste, mająca na celu przejęcie czyjeś tożsamości. 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.

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.

Atak DoS

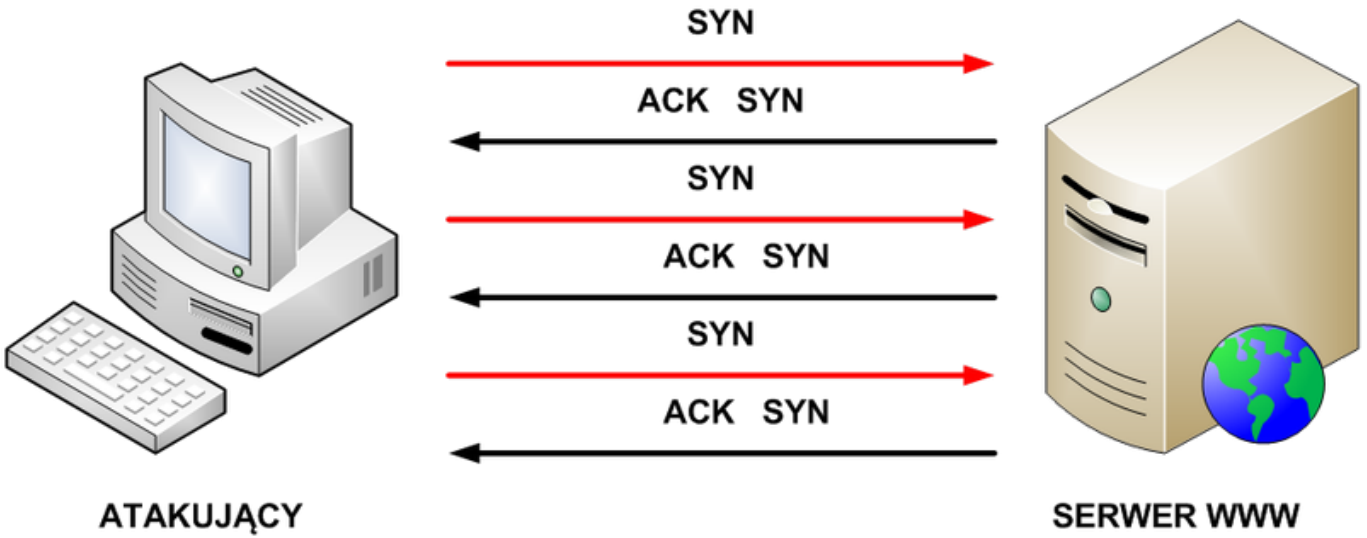


Ataki DoS (ang. Denial of Service) prowadzone są na pojedyncze komputery lub grupy komputerów i mają na celu uniemożliwienie korzystania z usług. Celem ataku DoS mogą być systemy operacyjne, serwery, routery i łącza sieciowe.

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.

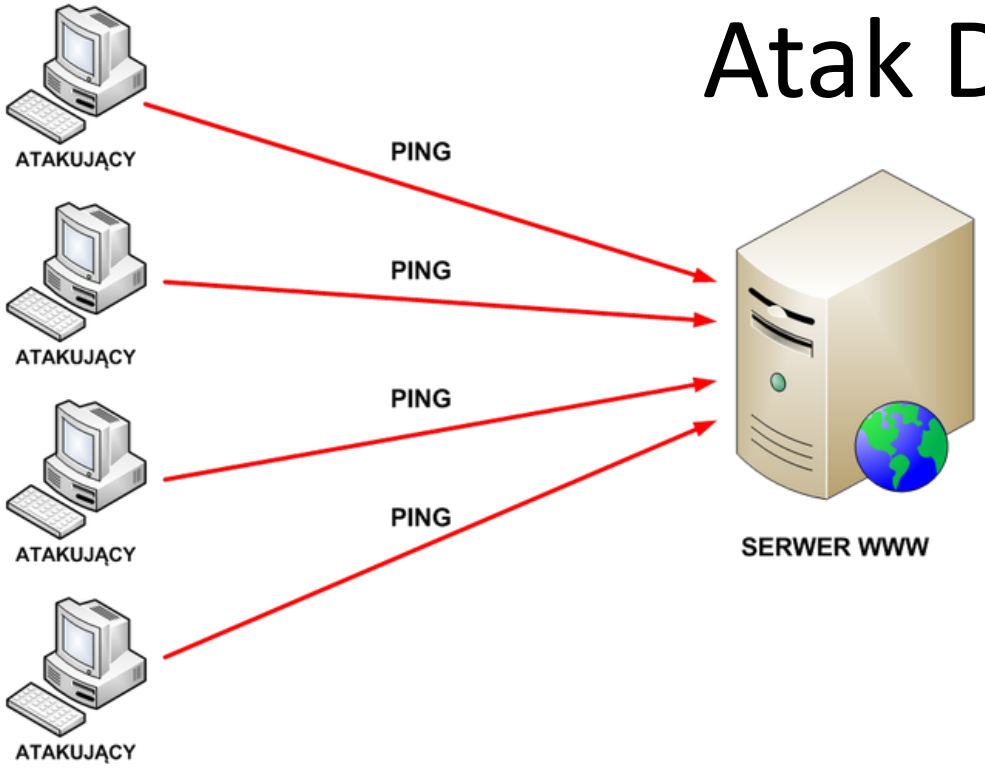
Atak DoS



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
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.

Atak DDoS



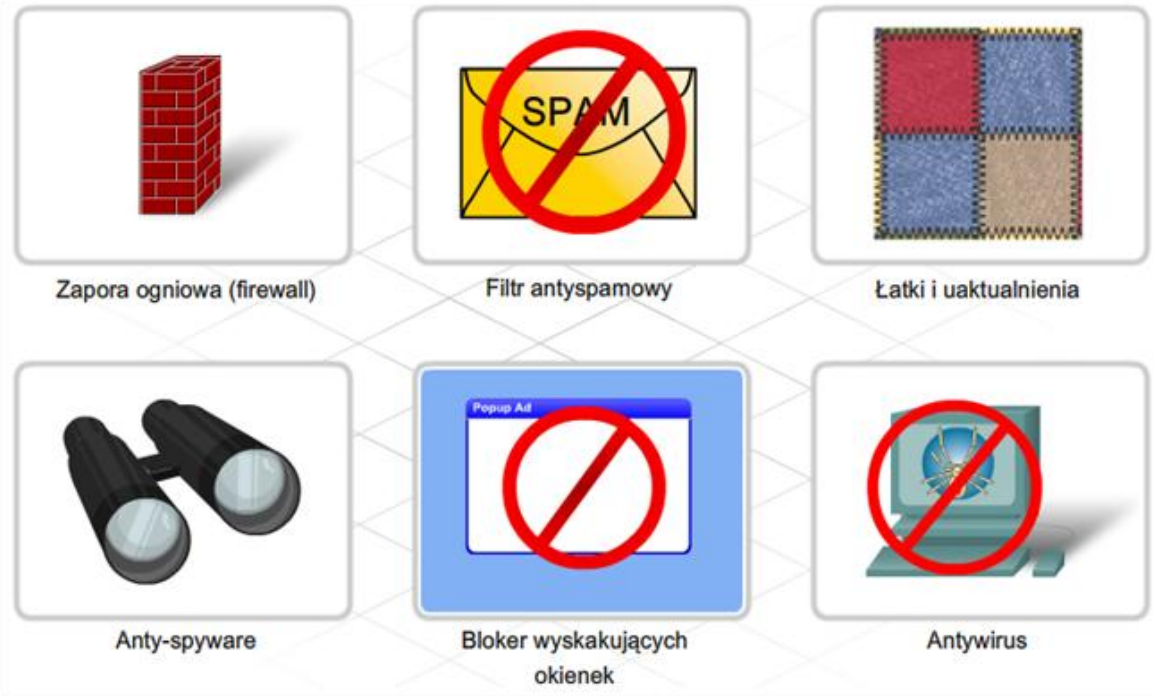
Atak DDoS (ang. Distributed Denial od Service) jest odmianą ataku DoS ale o wiele bardziej wyrafinowaną i potencjalnie bardziej szkodliwą. Został stworzony w celu nasycenia sieci bezużytecznymi danymi. DDoS działa na znacznie większą skalę niż ataki DoS. Zwykle atakuje setki lub tysiące miejsc jednocześnie. 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 .

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 dokonanie weryfikacji informacji (np. hasło, nazwa użytkownika), by rzekomo zabezpieczyć ofiarę przed groźnymi konsekwencjami.

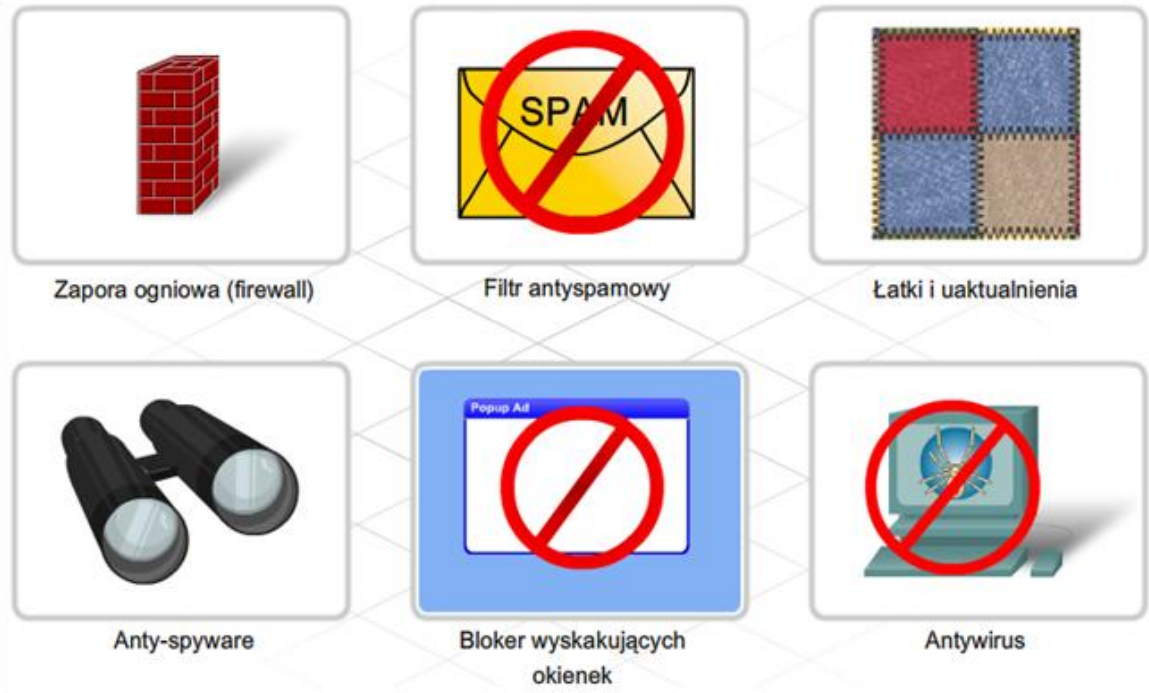
Narzędzia i aplikacje do zabezpieczenia sieci



Polityka bezpieczeństwa powinna być w centralnym punkcie procesów zabezpieczania, monitorowania, testowania i ulepszania sieci. Politykę realizują procedury bezpieczeństwa. Procedury te 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.

Narzędzia i aplikacje do zabezpieczenia sieci



Przykłady narzędzi i aplikacji używane do zabezpieczania sieci (rys. 30):

1. **Zapora ogniowa** – sprzętowe lub programowe narzędzie bezpieczeństwa, które kontroluje ruch do i z sieci.
2. **Blokery spamu** – oprogramowanie zainstalowane na serwerze lub komputerze użytkownika, identyfikujące i usuwające niechciane wiadomości.
3. **Łatki i aktualizacje** – oprogramowanie dodane do systemu lub aplikacji poprawiające 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.