Informatyka

Wirusy, ataki i sposoby zabezpieczeń…

(o chorobach trapiących komputery…)

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.

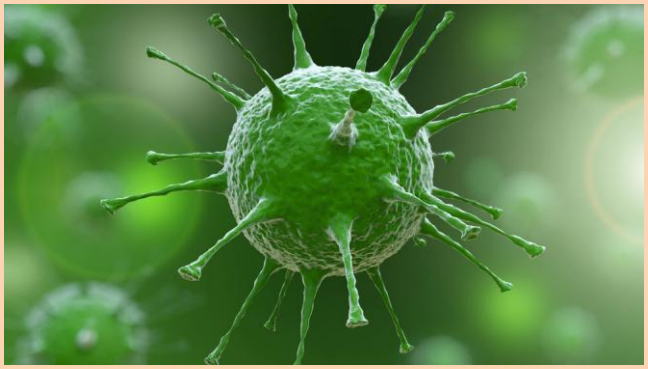
Czasem techniki te są używane w połączeniu z socjotechniką, aby oszukać nieostrożnego użytkownika, by ten nieświadomie uruchomił taki atak.

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.

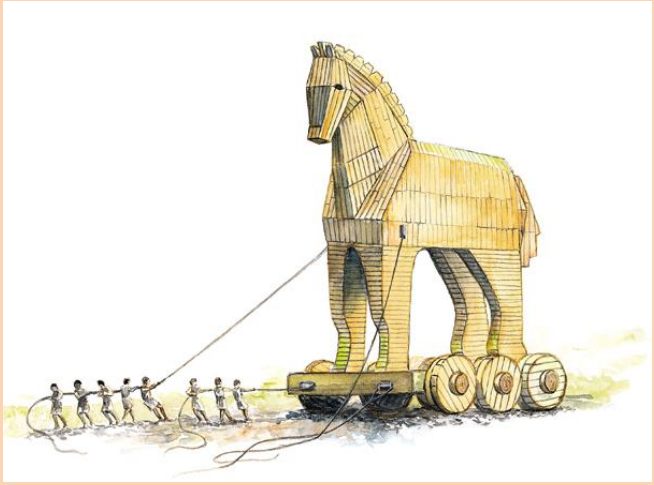
Nie wymagają aktywacji czy ludzkiej interwencji. Samorozprzestrzeniające się robaki sieciowe są o wiele groźniejsze niż pojedynczy wirus, gdyż mogą szybko zainfekować duże obszary Internetu.

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.

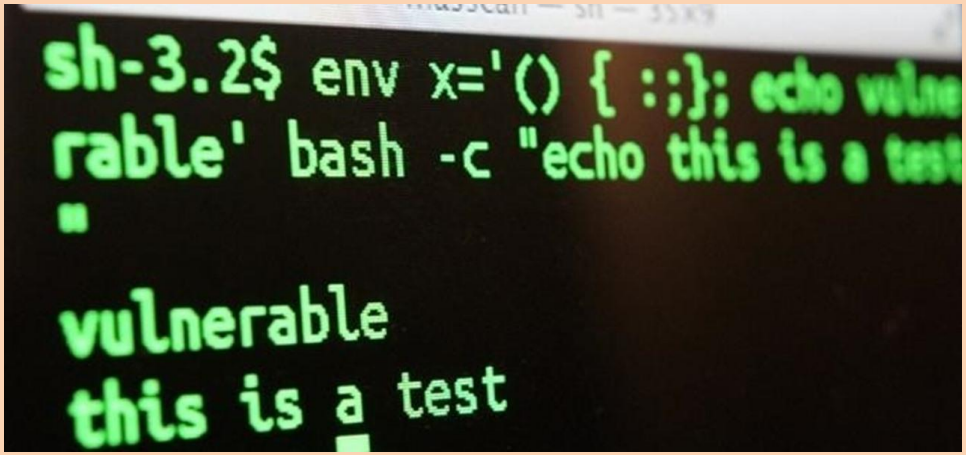


Bomba logiczna (ang. logical bomb)

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.

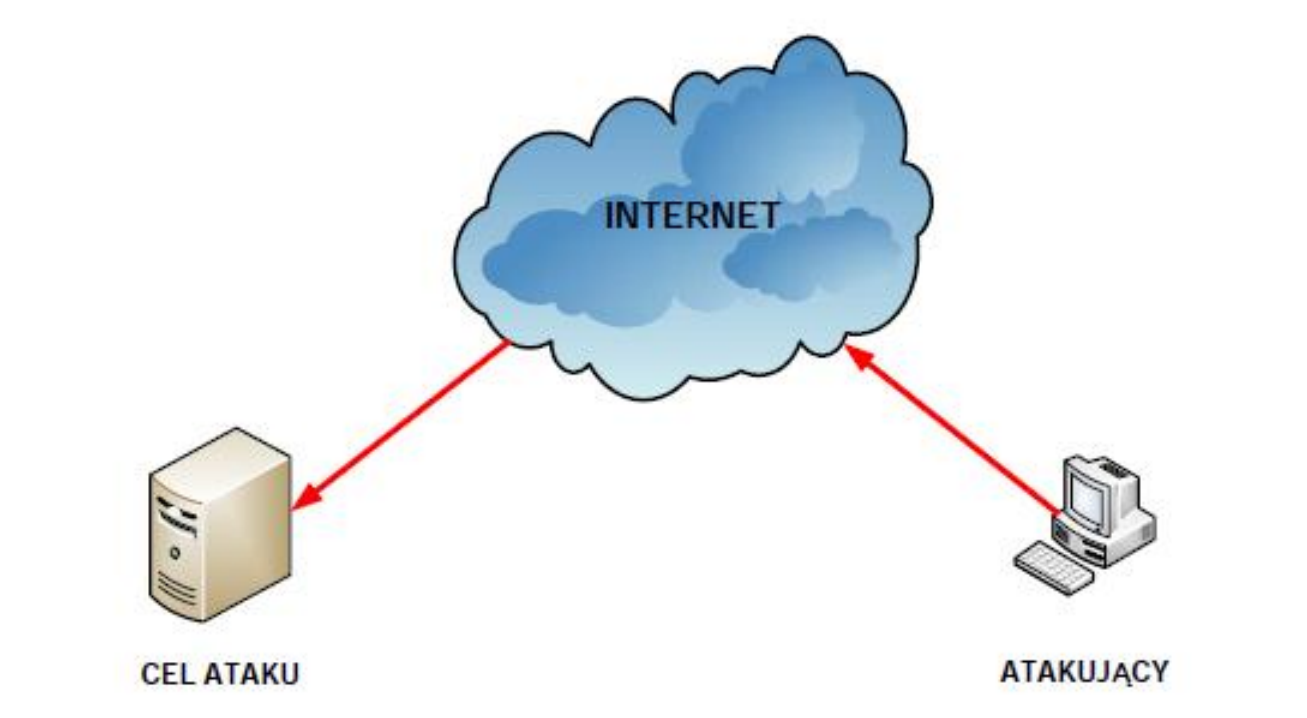
Stealware w przypadku stwierdzenia próby płatności przez Internet podmienia numer konta, na które zostaną wpłacone pieniądze.

ATAKI SIECIOWE

Atak zewnętrzny

Ten sposób złośliwego oddziaływania jest powodowany przez osoby, które nie pracują w danej organizacji.

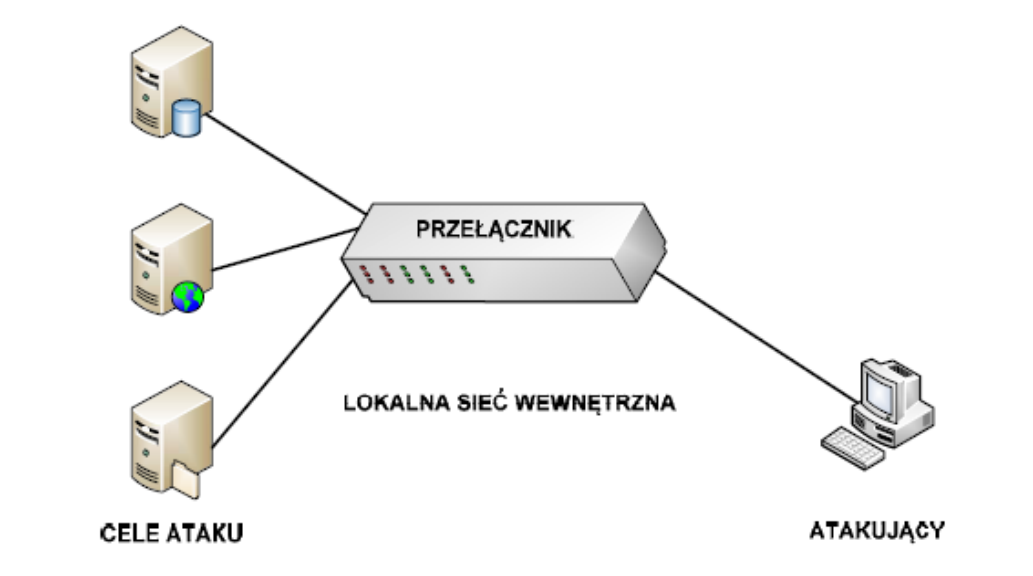
Atakujący z zewnątrz toruje sobie drogę dosieci głównie przez Internet.



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.

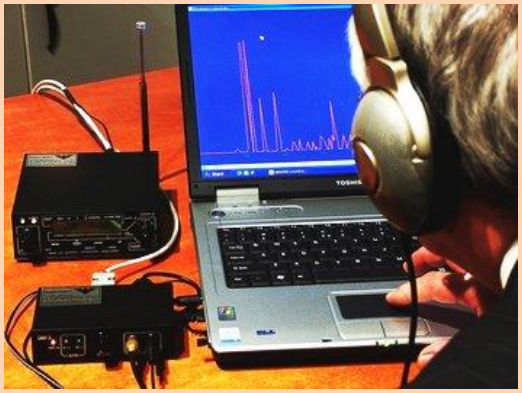


Podsłuch sieciowy (ang. sniffing)

Podstawowym zagrożeniem, z którym każdy może się spotkać jest nieuprawnione przechwycenie (podsłuchanie) danych.

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.



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.

WŁAMANIA

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.

ZABEZPIECZENIA

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.

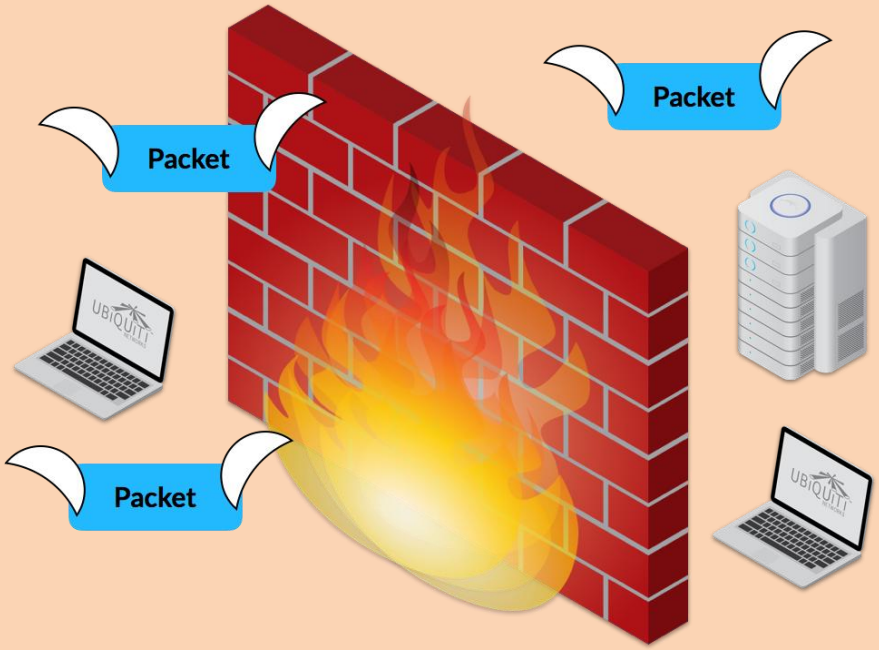
Mogą definiować kroki prewencyjne zmniejszające ryzyko jednocześnie informując, jak radzić sobie po stwierdzeniu naruszenia zasad bezpieczeństwa.

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:

0.Podstawowy poziom zabezpieczeń do aktualny i aktywny program antywirusowy

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.