Zagrożenia internetowe i bezpieczeństwo danych

TYP ZAGROŻEŃ INTERNETOWYCH

MALWARE

(złośliwe oprogramowanie) to nazwa określająca programy, których celem jest uszkodzenie systemu, zdestabilizowanie pracy komputera, przejęcie danych oraz wszelka działalność mogąca zaszkodzić użytkownikowi. Ze względu na obszar działania oraz sposób rozprzestrzeniania się, malware można podzielić na następujące kategorie:

TYP ZAGROŻEŃ INTERNETOWYCH

WIRUS KOMPUTEROWY

Jest to program, który działając bez wiedzy użytkownika wykonuje szereg operacji uniemożliwiających lub utrudniających poprawne działanie systemu operacyjnego. Wirusy przenoszone są poprzez zainfekowane pliki (nosiciela). Aby doszło do infekcji, plik-nosiciel wraz z wirusem muszą zostać dostarczone do docelowego komputera. Plik taki może zostać przesłany poprzez sieć Internet, przeniesiony za pomocą dyskietki, płyty CD lub DVD, pamięci USB lub innego nośnika danych. W zakres niepożądanych efektów związanych z obecnością wirusa w systemie wchodzą między innymi:

kasowanie, zmiana lub niszczenie danych;

uniemożliwianie pracy na komputerze;

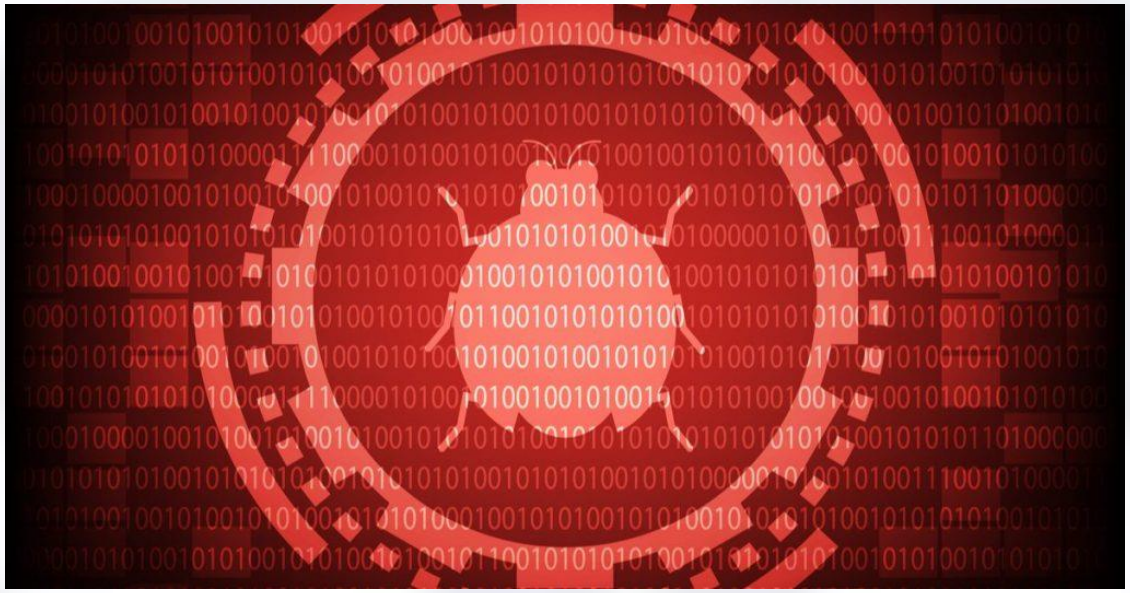
wyświetlanie niechcianych grafik lub odgrywanie dźwięków;

przejęcie kontroli nad komputerem osobie nieupoważnionej.

TYP ZAGROŻEŃ INTERNETOWYCH

ROBAK (WORM)

Robak, choć podobny do wirusa pod względem niepożądanego oddziaływania, jakie ma na komputer, różni się sposobem przenoszenia. Robak nie potrzebuje pliku nosiciela, rozprzestrzenia się poprzez sieć, w której znajduje się dany komputer.



TYP ZAGROŻEŃ INTERNETOWYCH

KOŃ TROJAŃSKI (TROJAN)

Trojan zwany też koniem trojańskim to program, który podając się za oprogramowanie znane i przydatne użytkownikowi, w rzeczywistości jest złośliwym oprogramowaniem. Uruchomienie trojana może nastąpić, poprzez otwarcie załącznika e-mail, uruchomienie pliku pobranego z sieci, lub odwiedzenie zainfekowanej strony.

TYP ZAGROŻEŃ INTERNETOWYCH

OPROGRAMOWANIE SZPIEGUJĄCE (spyware)

Oprogramowanie szpiegujące wykonuje określone działania bez wiedzy użytkownika. Zadaniem aplikacji spyware jest zbieranie informacji o użytkownikach np. sposobie korzystania z sieci oraz odwiedzanych stronach, jak również wykradanie poufnych danych, takich jak loginy oraz hasła dostępu do kont bankowych, serwisów aukcyjnych, sklepów internetowych, etc.

TYP ZAGROŻEŃ INTERNETOWYCH

ROOTKIT

Oprogramowanie, modyfikujące działanie systemu operacyjnego i ukrywające w ten sposób przed użytkownikiem pewne zdarzenia lub elementy, np. procesy, pliki czy połączenia sieciowe. Rootkity pozwalają na przejęcie maszyny przez osoby trzecie, które mogą następnie wykorzystać go do popełnienia przestępstwa np. ataku hakerskiego lub rozsyłania spamu.

TYP ZAGROŻEŃ INTERNETOWYCH

SPAM

to niechciane i niepotrzebne wiadomości elektroniczne przesyłane użytkownikowi.

Wiadomości takie rozsyłane są za pośrednictwem poczty elektronicznej, komunikatorów, oraz zamieszczane są na forach dyskusyjnych lub portalach społecznościowych.

Do charakterystycznych cech spamu należy jego skala. Wiadomości przeważnie przesyłane są masowo, do wielu losowo wybranych użytkowników. Przeważnie nadawca spamu nie jest znany użytkownikowi a treść wiadomości nie leży w obszarze zainteresowań, ani w żaden inny sposób nie jest powiązana z odbiorcą.

TYP ZAGROŻEŃ INTERNETOWYCH

PHISHING

jest formą ataku opartego na inżynierii społecznej, mającego na celu uzyskanie loginu, hasła lub innych danych użytkownika.

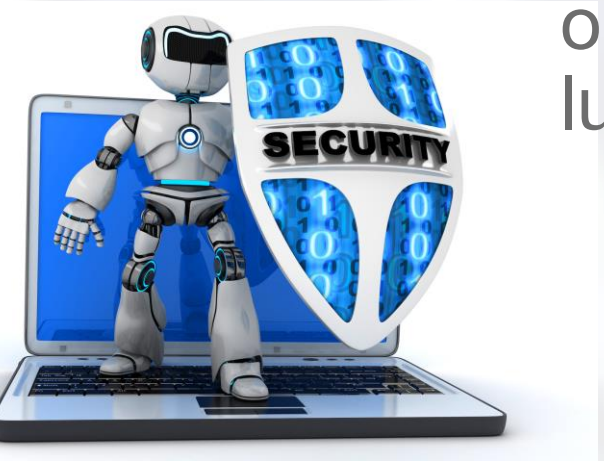
Aby tego dokonać, atakujący podszywają się pod znaną ofierze osobę lub instytucję i proszą o podanie informacji lub wykonanie określonej czynności, np. zalogowanie się na zainfekowanej stronie lub odwiedzenie wskazanego adresu WWW.

Phishing stosowany jest przeważnie w celu pozyskania danych, które mogą zostać wykorzystane dla osiągnięcia korzyści majątkowych. Celem atakujących są głównie loginy i hasła do kont bankowych, numery kart kredytowych, hasła jednorazowe czy dane osobowe.

ZABEPIECZENIA

Stosowanie oprogramowania zabezpieczającego komputer w dzisiejszych czasach jest konieczne. Codziennie w internecie pojawia się 17 000 aplikacji, będących zagrożeniem dla naszych komputerów.

Przestępczość komputerowa jest najszybciej rosnącym segmentem IT. Niestety nadal wielu użytkowników w ogóle nie posiada oprogramowania zabezpieczającego lub to, które posiada jest nieaktualne.



ANTYWIRUS

Oprogramowanie antywirusowe potocznie nazywane antywirusem, jest narzędziem chroniącym komputer przed złośliwym oprogramowaniem. Antywirus posiada funkcje zapobiegania i przeciwdziałania infekcjom wirusów, robaków, trojanów itp. Programy antywirusowe poza funkcjami diagnostycznymi umożliwiają także usuwanie złośliwego oprogramowania z systemu.

Aby antywirus spełniał swoja rolę, konieczne jest aktualizowanie bazy definicji wirusów oraz regularne przeprowadzanie skanowania systemu. Większość programów antywirusowych można skonfigurować tak, by te czynności wykonywały się automatycznie.

FIREWALL

Firewall (w jęz. polskim występuje także pod nazwą zapora sieciowa i zapora ogniowa) jest to osobne urządzenie lub program, którego zadaniem jest monitorowanie ruchu sieciowego przechodzącego przez niego i w zależności od ustawień blokowanie lub przepuszczanie dalej. Firewall przeważnie znajduje się pomiędzy dwoma obszarami sieci, np. pomiędzy obszarem bezpiecznym – komputerem użytkownika i siecią zewnętrzną - Internet. W ten sposób wszystkie próby połączenia z komputerem oraz komputera z siecią zewnętrzną będą musiały przejść przez firewall. Poprzez szereg ustawień i reguł niepożądany ruch sieciowy zostanie wykryty i zablokowany.

AKTUALIZACJE

Ponieważ złośliwe oprogramowanie wykorzystuje luki w systemie i oprogramowaniu zainstalowanym na komputerze bardzo ważne jest regularne sprawdzanie czy istnieją dostępne łatki, usuwające błędy. Tak samo ważne jest aktualizowanie oprogramowania chroniącego komputer. By jak najlepiej chronić komputer i dane należy sprawdzać czy dostępne są definicje najnowszych wirusów. Większość oprogramowania posiada funkcje automatycznej aktualizacji, dzięki której użytkownik może usprawnić powyższy proces.

ZAUFANE ŹRÓDŁA

Aby zmniejszyć ryzyko zainstalowania złośliwego oprogramowania na komputerze należy zachowywać szczególną ostrożność w przypadku programów pobieranych z Internetu. Zalecane jest instalowanie oprogramowania jedynie z zaufanych i znanych źródeł oraz nie instalowanie oprogramowania, na które wskazują odnośniki w mailach przesłanych od nieznanych nadawców.

Zapraszam do zadawania pytań

Dziękuję za uwagę
Waldemar Serafin