ZAGROŻENIA SIECI KOMPUTEROWYCH

Rodzaje zagrożeń

Do najpoważniejszych zagrożeń należą:

- podszywanie;
- modyfikacja;
- odmowa usługi;
- wirusy;
- złośliwe oprogramowanie;
- luki i dziury w systemie.

Podszywanie - Stacja nieautoryzowana udaje inną stację autoryzowaną, w celu zdobycia niejawnych informacji.

Modyfikacja - Zmiana treści danych, np. podczas transmisji.

Odmowa usługi - stacja nie spełnia swoich funkcji z powodu zniszczenia system lub zajęcia całej dostępnej pamięci oraz gdy stacja uniemożliwia właściwą pracę innych stacji przez likwidowanie komunikatów czy generowanie sztucznego ruchu. Skuteczne uniemożliwienie świadczenia usług w sieci nazywamy atakiem typu **DoS** (*ang. Denial of Service*). Istnieje nowsza wersja ataku DoS jest to **DDoS** (*ang. Distributed Denial of Service*) – czyli rozproszona odmowa usługi, polegający na tym, że atakujące pakiety przychodzą z dziesiątek czy nawet setek różnych źródeł jednocześnie.

Wirusy

Wirus komputerowy to złośliwy program, którego kod wykonywalny zaszyty jest w innym programie użytkowym lub w inny sposób jest z nim powiązany. Żądanie uruchomienia programu powoduje, że wykonywane są instrukcje wirusa a potem dopiero kod programu.

Sposób infekcji i rezydowania wirusów wyznacza ich podział na:

- dyskowe,
- plikowe,
- towarzyszące,
- sprzęgające,
- hybrydowe

- rezydentne,
- nie rezydentne,
- mieszane (hybrydowe).

Zadania wirusów:

- powielanie własnego kodu i umieszczanie go w określonych miejscach na dyskach lub w programach,
- niszczenie lub zmiana zapisanej na dyskach informacji,
- generowanie dziwnych komunikatów i melodii itp.,
- zakłócanie wyświetlania informacji na ekranie,
- próby fizycznego uszkodzenia sprzętu.

Wirus dyskowy podmienia zawartość głównego sektora ładowania, przenosi się przez fizyczną wymianę każdego nośnika pamięci. Dysk systemowy zostaje zainfekowany wirusem sektora ładowania tylko wtedy, gdy użytkownik uruchomi systemu z zainfekowanego nośnika.

Wirus plikowy modyfikuje zawartość plików wykonywalnych (COM, EXE, SYS i innych). Integruje się z plikiem pozostawiając nienaruszoną większą część jego kodu, a wykonywanie programu odwraca w taki sposób, że kod wirusa wykonuje się jako pierwszy, a dopiero potem następuje uruchomienie zarażonego programu, który najczęściej nie zostanie uruchomiony.

Wirus towarzyszący. Działa na tej zasadzie, że z dwóch programów o tej samej nazwie, system operacyjny wykonuje plik z rozszerzeniem *.COM przed plikiem *.EXE. Wirus towarzyszący tworzy plik z rozszerzeniem *.COM i umieszcza w nim swój własny kod wykonywalny a nazwa pliku jest taka sama jak plik z rozszerzeniem *.EXE.

Wirus sprzęgający. Wirus sprzęgający nie modyfikuje plików ale mimo to jest bardzo żywotny i w szybkim tempie się mnoży. Wirus sprzęgający dołącza do pierwszego wskaźnika JAP'a katalogu zapisu każdego pliku wykonywalnego do pojedynczego JAP'a zawierającego swój własny kod.

Właściwy numer pierwszego JAP'a zainfekowanego pliku jest przechowywany w nieużywanej części zapisu katalogu. Wirusów tego typu powstało bardzo mało. Przykładowy wirus: DIR-2.

Wirus hybrydowy. Wirus hybrydowy jest krzyżówką wyżej wymienionych wirusów łączący w sobie ich metody działania. Najbardziej spotykane jest łączenie wirusa sektora ładowania z wirusem pasożytniczym plikowym, co w konsekwencji daje to największe możliwości replikacji a jednocześnie utrudnia usunięcie wirusa z systemu.

Wirus rezydentny. Ładują się do pamięci jako rezydentne programy usługowe i przejmują jedno lub więcej przerwań. Do infekcji dochodzi w wyniku spełnienia ściśle określonych warunków, przykładowo uruchomienie programu.

Wirus nie rezydentny. Uruchamia się wtedy, gdy jest wykonywany zarażony program. Wykonuje on całkowicie swój program nie pozostawiając po sobie śladów w pamięci komputera – nie rezyduje w pamięci.

Wirus mieszany. Po zainfekowaniu systemu i uzyskaniu kontroli wirus mieszany korzysta z metod działania wirusów rezydentnych jak i nie rezydentnych. Początkowo działa jak wirus nie rezydentny a po uzyskaniu pełnej kontroli pozostawia w pamięci rezydentny fragment swojego kodu.

Złośliwe oprogramowanie

- konie trojańskie,
- bomby logiczne,
- ukryte narzędzia zdalnej administracji – backdors,
- programy kradnące hasła i inne poufne informacje - backdors,
- programy w przyszłości mające być wirusami,
- zestawy do konstruowania wirusów i generatory polimorficzne.

Koń trojański zawiera kod realizujący funkcje inne niż te, o których mowa jest w załączonej dokumentacji. Może być dowolny program np. do słuchania stacji radiowych z dołączonym kodem, który po 8 godzinach pracy dokona spustoszeń na dysku systemowym poprzez kasowanie lub po prostu formatowanie dysku. Konie trojańskie najczęściej niszczą dane na dyskach lub zawieszają pracę systemu w zależności od pewnych okoliczności lub przy pierwszym uruchomieniu. Konie trojańskie najczęściej zaszyte są w programach „imitujących" inne użyteczne narzędzia lub jako uaktualnienie do niego. Nie rozpowszechniają się błyskawicznie gdyż same ulegają destrukcji przy niszczeniu danych na dyskach lub ujawniają swoją obecność i są kasowane przez użytkowników. ***Backdoors.*** Jest specyficznym rodzajem konia trojańskiego i odmmiennym sposobem działania. Służy hakerom jako narzędzie do zdalnej administracji.

Bomba logiczna. Złośliwy kod bomby logicznej umieszczony w programie, który uaktywni się tylko wtedy, gdy spełnione zostaną ściśle określone warunki np. kod destrukcji systemu po usunięciu nazwiska z listy płac. W przypadku koni trojańskich, które wykonują destrukcyjną działalność od razu po uruchomieniu lub z niewielkim opóźnieniem, o tyle bomba logiczna by dokonać zniszczeń w systemie czeka na spełnienie ściśle określonych warunków, np. określonej daty, liczby uruchomień.

Robak. Program, który w sposób nie kontrolowany mnoży się w zasobach sieci komputerowej a jego działanie sprowadza się do tworzenia własnych duplikatów. W odróżnieniu od innych wirusów nie atakuje on żadnych plików. Oprócz uszczuplania wolnego miejsca na dysku program ten rzadko wywołuje inne niepożądane skutki uboczne.

Królik. Program wykorzystujący w pełni określone zasoby systemu a na skutek błyskawicznego i nie kontrolowanego powielania się zapełnia system.

Makrowirusy. Makrowirusy umieszczane są w definicjach makr w plikach tekstowych najpopularniejszych aplikacji, dla przykładu mogą to być: Visual Basic for Applications w programie Microsoft Excel lub Word Basic w Microsoft Word.

Luki i dziury w systemie

Exploity są to programy wykorzystujące wszelkie luki i błędy w systemach operacyjnych i oprogramowaniu.

Exploity dzielimy na następujące kategorie:

- pozwalające uzyskać prawa użytkownika, w tym administratora (*tzw. rootkiy- zakorzenić się i zdobyć pozycję*);
- powodujące atak na odmowę usługi (*ang. DoS denial of service*);
- umożliwiające atak przez podszywanie się pod adres IP (*ang. IP spoofing*).

Rootkiy. Eksploity dające dostęp do systemu, są bardzo groźne. Wykorzystują błędy w sposobie implementacji protokołu TCP systemu, a „przepełnienie" bufora pozwala na zamazanie części plików, a dokładnie pierwszej linii pliku z zakodowanymi hasłami, gdzie przechowywane jest hasło administratora. Przy pomocy exploitów pozwalających wykorzystać te luki haker jest w stanie przejąć połączenie, uzyskać zdalnie konto na serwerze, po czym uaktywnić powłokę i wykonywać czynności na prawach lokalnego użytkownika sieci a nawet przejąć prawa administratora.

Atak DoS. Wszelkiego rodzaju ataki prowadzące do blokady usług sieciowych:

- *nuke*;
- „zapychanie" portów;
- atak typu *land*;
- *ping* śmierci;
- TCP SYN;
- atak typu *smurf*;
- atak typu *Distributed Denial of Service* (DDoS).

Ataki typu *nuke* – występują w systemach Microsoft Windows, efektem wizualnym tego ataku jest niebieski ekran z komunikatem błędu i konieczność restartu systemu.

„**Zapychanie**" portów spowodowane jest przez hakera, który przy pomocy specjalnych programów wysyła lawinę prób połączenia z określonym portem komputera i powoduje całkowite zablokowanie transmisji.

***Ping* śmierci** – „zapingować na śmierć". Haker wysyła bardzo dużą ilość zapytań czy dany host jest w sieci, przez co atakowany komputer nie jest w stanie robić nic innego jak tylko na nie odpowiadać.

Atak typu *land* – atakujący podszywa się pod adres IP i wysyła do ofiary pakiety TCP, gdzie adres źródłowy i adres docelowy pakietu są takie same. Zaatakowany serwer zaczyna odpowiadać sam sobie a próba nawiązania takiej transmisji absorbuje go całkowicie przez co nie jest zdolny do jakiegokolwiek innego działania.

Atak TCP SYN – dla połączeń TCP rezerwowana jest taka ilość pamięci, że nie pozostaje jej wystarczająco dużo dla innych funkcji. Podczas nawiązywania transmisji w protokole TCP pomiędzy dwoma komputerami, strona inicjująca połączenie wysyła pakiet z ustawioną flagą SYN – czyli żądaniem rozpoczęcia synchronizacji transmisji, zaś druga strona po jego odebraniu wysyła pakiet z flagą ACK, czyli potwierdzeniem. Po otrzymaniu potwierdzenia przez inicjatora powinna rozpocząć się transmisja danych. Haker jednak wysyła tylko i wyłącznie pakiety z żądaniem synchronizacji bez przesłania właściwych danych, przez co zmusza ofiarę do odpowiedzi pakietem ACK na każde żądanie.

Smurfing – zalanie sieci takim ruchem nadawczym, zę w sieci pojawiają się zatory. Polega to na wykorzystaniu routerów, które w swej konfiguracji nie sprawdzają pochodzenia pakietów. Haker wysyła pakiet ICMP (*ang. ping*) do ofiary ze zmodyfikowanym adresem źródłowym, który wskazuje na wykorzystywany router a nie host atakującego. Ofiara odpowiadając odsyła pakiet ICMP do routera, a ten z kolei wysyła go do wszystkich hostów w sieci, których ruchem kieruje, te zaś wszystkie odpowiadają „pingując" ofiarę. Wielkość sieci przekłada się na skuteczność tego typu ataku, im większą sieć kontroluje router (nazywany wzmacniaczem smurfowym – *ang. smurf amplifier*), tym atak jest skuteczniejszy. Trudno jest chronić się przed smurfingiem, a jedynym wyjściem jest ograniczenie liczby wzmacniaczy – routerów, które nie sprawdzają pochodzenia pakietów.

Spoofing – to podszywanie się pod innego hosta sieci. Intruz, któremu uda się podszyć pod autoryzowany host, wysła wiadomość ze sfałszowanym adresem poczty elektronicznej a w przesłanych danych dołącza konia trojańskiego, którego uruchomienie spowoduje przeszukanie dysku serwera w celu odszukania pliku z kontami i hasłami użytkowników a w konsekwencji wysłanie informacji zwrotnych na adres fałszywego nadawcy.

Podobne działania hacker podszywający się pod adres serwera WWW. Intruz przekazuje informację do atakowanego serwera z prośbą o przysłanie odpowiedniej strony WWW, a następnie przesyła ją prawdziwemu adresatowi. W trakcie przesyłania intruz podmienia prawdziwą stronę na fałszywą. Zatem prawdziwy adresat otrzymuje już fałszywą informację. Działanie tego typu jakim jest podszywanie się pod inne serwisy określa się jako ***fishing*** [18]. Należy pamiętać, że jeśli dostaniemy e-maila pochodzącego rzekomo z serwisu, z którego często korzystamy i mamy do niego zaufanie w żadnym razie nie „klikamy" na linki. Po wybraniu takiego linku trafimy na podmienioną stronę np. fikcyjną stronę serwisu Allegro gdzie możemy skusić się na kupno fikcyjnych towarach.

Skanowanie portów – przy pomocy odpowiedniego oprogramowania można wyszukiwać luk w otwartych portach aplikacji komunikujących się z Internetem. Taka obserwacja pozwala na poznanie wszystkich usług udostępnianych przez system i wyselekcjonowanie potencjalnie najsłabiej chronionych w celu późniejszego ataku. Profesjonalne skanery portów służą jako narzędzia do testowania bezpieczeństwa systemu i powinny być okresowo stosowane przez administratorów sieci.

Rodzaje ataków

Z punktu widzenia bezpieczeństwa możemy wyróżnić dwa rodzaje ataków:

- ataki pasywne;
- ataki aktywne.

Ataki pasywne czyli zagrożenia bierne rozumiane są jako przechwycenie danych i ich treści lub sama analiza ruchu.

Ataki aktywne dzielimy na:

- przerwanie;
- modyfikacja;
- podrobienie.

Ataki aktywne czynnie zagrażają sieci. Dochodzi do bezpośredniego oddziaływania na sieć, nieautoryzowanych zmian w systemie, kasowania i destabilizacji pracy aplikacji sterujących, modyfikacji, powtórzeń lub podmianie treści wiadomości na fałszywe informacje.

Podział intruzów

Haker. Narusza bezpieczeństwo sieci w celu potwierdzenia swoich umiejętności lub okazania dezaprobaty atakowanej instytucji. Nie jest nastawiony na czerpanie korzyści a szkody jakie wyrządzi zależą od jego etyki.

Szpieg. Atakuje w celu uzyskania ważnych informacji politycznych, gospodarczych i wojskowych. Kradnie ważne dane strategiczne i militarne, nowe technologie, tajemnice państwowe i nie tylko. Stara się zatrzeć ślady swojej działalności.

Terrorysta. Atakuje w celu osiągnięcia korzyści politycznych i propagandowych. Jego działalność jest destrukcyjna i prowadzi do zastraszenia i wywołania paniki.

Nieuczciwy pracownik. W celu osiągnięcia korzyści finansowych lub z powodu innych pobudek osobistych udostępnia dane, tajemnice, strategie i wszelkie inne poufne informacje dla konkurencji. Działając na szkodę firmy stara się nie pozostawić żadnych śladów swej przestępczej działalności.

Zawodowy przestępca. To wąska grupa atakujących sieci o szerokiej gamie działalności w celu uzyskania korzyści materialnych. Kopiują zasoby systemu, raczej nie kasują i nie modyfikują informacji.

Wandal. Bardzo szeroka grupa atakujących. Dokonują zniszczenia poprzez kasowanie lub wszelkiego rodzaju podmiany stron często nie lubianych przez siebie organizacji w celu zamanifestowania swego niezadowolenia i nie tylko.

Voyeur. Atakuje dla podniesienia adrenaliny we krwi i napawania się strachem z samego faktu poznania niejawnych informacji. Czasami kopiuje dane by zapoznać się z nimi później. Stara się nie czynić żadnych strat w systemie ani zmian w kopiowanych danych.

Innym rodzajem podziału atakujących jest źródło ich pochodzenia:

- zewnętrzne
- wewnętrzne

Internet

Poczta elektroniczna

Głównym źródłem i drogą infekcji wirusami jest poczta elektroniczna. W przypadku zarażenia jednego z komputerów infekcja rozprzestrzenia się i wirusy rozsyłane są do kolejnych odbiorców znajdujących się w książce adresowej programu pocztowego. Hakerzy licząc na naiwność odbiorców, zaczęli wysyłać wirusy poczta elektroniczną. I o dziwo nie zawiedli się, czego przykładem są: Melissa – jeden z pierwszych wirusów rozsyłających się przez e-maile, który potrafił w ciągu godziny przenieść się do ponad 5tys. komputerów; kolejne sławne wirusy to I Love You i Anna Kurnikowa, które przekroczyły 6tys. infekcji na godzinę, a Code Red i Nimda zbliżyła się do granicy 7tys.

Innym popularnym wykroczeniem w sieci jest mailbombing, czyli bomba z adresem nadawcy. Intruz atakuje adres odbiorcy dużą liczbą przesyłek i w krótkim czasie doprowadza do zapchania jego skrzynki pocztowej.

Na podobnej zasadzie działa spam – czyli nie chciana poczta.

Infrastruktura sieci w Bejrucie

Ciasteczka

Cookies to pliki z krótkim opisem przesyłanym przez serwer Webu i zapisywanych przez przeglądarkę na dysku lokalnym. Przy ponownym uruchomieniu i wczytaniu przez nią plików *cookie* do pamięci serwer Webu rozpoznaje klienta i zwraca określony rodzaj informacji. Ciasteczka usprawniają prace nawigacyjną w Webie, identyfikują, przechowują wszelkiego rodzaju informacje typu: hasła, ustawienia stron, profile itp. Nie ma jednak żadnych podstaw i niebezpieczeństwa by cookies pozwalały ujawnić serwerowi struktury katalogów i danych zapisanych na dysku w komputerze klienta. Serwer może odczytać tylko to co sam zapisał, do pozostałych katalogów nie ma dostępu.

Java

Język Java powstał w firmie Sun Microsystems jako narzędzie do programowania w graficznym środowisku sieciowym. Jest wykorzystany do tworzenia tzw. Atletów czyli miniaplikacji, które są zagnieżdżone w dokumentach HTML i uruchamianych przez przeglądarkę na maszynie klienta. J

Aplety to niewielkich rozmiarów programy wywoływane w przeglądarkach drogą zagnieżdżania w dokumentach HTML i wykonywane komputerze kliencie.

Aplikacja jest normalnym programem, który nie wymaga przeglądarki oraz mechanizmu sprowadzającego je z serwera jak w przypadku apletu, z tą różnicą, że może pracować na dowolnej platformie wyposażonej w JVM.

Przed uruchomieniem, kod bajtowy Javy jest weryfikowany przez weryfikator kodu bajtowego, który sprawdza czy:

- nie fałszuje on wskaźników,
- nie narusza ograniczeń dostępu,
- uzyskuje dostęp do obiektów wyłącznie zgodnie z ich przeznaczeniem.

Jednak jak to bywa w praktyce nie ma produktów doskonałych a wszelkie usterki mogą być zauważone dopiero w czasie normalnej eksploatacji produktu. Możliwe jest napisanie appletu, który będzie zapisywał, kasował czy też modyfikował zbiory dzięki temu, że interpretator języka Java nie sprawdza do końca autentyczności informacji, możliwa jest podmiana bibliotek dynamicznych omijających restrykcyjność dostępności do katalogów. Rozwiązaniem są jak zwykle „łaty” producenta, oraz korzystanie z autoryzowanych bibliotek.

ActiveX

ActiveX to technologiia opracowana do lepszej współpracy aplikacji Windows przez Internet.

W jej skład wchodzą:

- ActiveX Controls,
- ActiveX Documents,
- Active Scripting,
- ActiveX Conferencing,
- Active Server.

ActiveX bazuje na standardzie COM (*ang. Component Object Model*) który definiuje warunki i metody współpracy różnych modułów aplikacji uruchomionych na pojedynczym komputerze, który wraz z OLE stał się fundamentem systemu Windows.By zapewnić minimalny poziom bezpieczeństwa Microsoft wymóg by autorzy kontrolek rejestrowali swoje wyroby w firmie YeriSign i zaopatrywali je w podpis elektroniczny gwarantując bezpieczeństwo danego produktu. Nie daje to jednak gwarancji pełnego bezpieczeństwa a mówi tylko jedynie kto jest autorem zarejestrowanej kontrolki.

Najlepszym podejściem jest korzystanie ze sprawdzonych i chronionych serwerów WWW, które nie dostarczają komponentów zainfekowanych wirusami lub w inny sposób niszczącymi system.