IDENTYFIKOWANIE ZAGROŻEŃ W SIECIACH KOMPUTEROWYCH

Na samym początku musimy zastanowić się, co znaczą słowa: zagrożenie sieci komputerowej. Zagrożenie, czyli coś co może wpłynąć niekorzystnie na naszą sieć. Naszym zadaniem jest zmniejszyć prawdopodobieństwo tego zdarzenia do jak najniższego poziomu. No tak, ale jeśli tak postąpimy to ograniczymy funkcjonalność i dostęp z naszej sieci do innych zasobów. Możemy np. całkowicie odłączyć się od Internetu, ale czy właśnie o to nam chodzi. Raczej w tej sytuacji należy przyjrzeć się sieci, którą należy zabezpieczyć, ale pod takim kątem, aby móc wyważyć między dostępem do niej, a jej bezpieczeństwem.

Najważniejsze co powinno być chronione w sieci komputerowej to informacja, bowiem celem wszelkich działań z zakresu bezpieczeństwa teleinformatycznego jest ochrona informacji, a nie sprzętu komputerowego. Brak takiego jasnego priorytetu ochrony niekiedy sprawia, że zasoby komputerowe są chronione w lepszy sposób niż informacja na nich przechowywana.

Najlepiej powinny być strzeżone informacje wrażliwe (istnieją jeszcze informacje niewrażliwe), które charakteryzują się tym, iż dla określonego podmiotu mogą być wykorzystane przeciwko niemu, jeśli dostaną się w niepowołane ręce.

Sam termin bezpieczeństwa teleinformatycznego definiuje się jako poziom uzasadnionego zaufania, że straty wynikające z manipulowania danymi nie zostaną poniesione. Informacja posiada trzy cechy odnośnie jej bezpieczeństwa, są to:

tajność – czyli stopień ochrony informacji, ustalana przez osoby posiadające informację; z pojęciem tym związana jest też poufność, czyli możliwość decydowania o przekazaniu informacji innej osobie lub możliwość przyjęcia danej informacji

integralność – oznacza, że informacja nie została w jakiś sposób zmodyfikowana

dostępność – bardzo charakterystyczna cecha w sieciach komputerowych zwłaszcza, oznacza możliwość skorzystania z danych przez uprawnionych użytkowników, aplikacji, procesów.

Innym atrybutem także mogącym się kwalifikować do tego zestawienia i często w takim wypadku podawany jest rozliczalność, czyli możliwość sprawdzenia, z jakich zasobów korzystał dany użytkownik.

Generalnie zagrożenia można podzielić na dwie kategorie: wewnętrzne i zewnętrzne. Zagrożenia wewnętrzne pochodzą z wewnątrz sieci mogą je powodować pracownicy firmy sabotujący działalność sieci.

Natomiast źródłem zagrożeń zewnętrznych są hosty pracujące poza naszą siecią, a w dobie Internetu o nie nie trudno. Najbardziej

spektakularne są włamania z zewnątrz, ponieważ są dużo trudniejsze do przeprowadzenia oraz firma odbiera taki napad jakby ktoś obcy wdarł się na jej podwórko. Najczęstsze jednak i te najbardziej niebezpieczne to przeprowadzane od wewnątrz. Nie mają one aż tak dużego rozgłosu, ponieważ firmy uważają, że pracownik dokonujący dzieł zniszczenia bądź utrudnienia pracy działania sieci to jej wewnętrzna sprawa. Należy jednak o nich cały czas pamiętać i bacznie zwracać uwagę na duże niebezpieczeństwo pochodzące od strony środka sieci.

Zagrożenia stwarzają intruzi, których można podzielić na dwie grupy ludzi.

Intruzi mający małą wiedzę z zakresu informatyki i niewielkie umiejętności. Najczęściej plan ataku czerpią z gotowych stron internetowych, dokumentów, bądź wiedzy swych kolegów. Stwarzają oni zagrożenia zwane niestrukturalnymi, ponieważ ich działania nie są w jakiś specjalny sposób uporządkowane i zaplanowane. Ale dlatego też atak może przynieść zaskakujące rezultaty. Jednakże ataki tego typu nie są zbyt trudne do wykrycia.

O wiele bardziej niebezpieczne są zagrożenia strukturalne, których źródłem są ludzie będący specjalistami w dziedzinie informatyki i którymi kieruje najczęściej chęć zysku lub silna motywacja do przekroczenia jakiejś bariery bezpieczeństwa. Są trudniejsze do wykrycia, ponieważ atakujący wiedzą jak zacierać za sobą ślady obecności.

Oba typy zagrożeń są niebezpieczne z tym, że ataków strukturalnych jest dużo mniej. Dla przykładu jednym z powszechnych zagrożeń niestrukturalnych jest człowiek próbujący odgadnąć hasło administratora na serwerze linuxowym.

Najbardziej podstawową ochroną przed sieciowym napadem jest ochrona fizyczna. Co oznacza, że musimy dobrze zabezpieczyć nasze fizyczne urządzenia sieciowe, aby niepowołana osoba nie miała do nich dostępu. Do kategorii tej zalicza się również elementy pasywne takie jak przewody, łączówki itp. Bardzo częsty i poważny błąd to sieć bezpieczna tylko w środowisku programowym, sprzętowym. Cóż nam bowiem z najlepszych urządzeń bezpieczeństwa, gdy złodziej ukradnie dysk twardy serwera, albo po prostu odłączy urządzenia sieciowe od prądu, bądź przerwie kabel sieciowy. Dlatego bardzo ważne jest umieszczenie urządzeń sieciowych w zamykanych pomieszczeniach, gdzie nie ma dostępu nikt poza dobrze znanymi nam pracownikami. Podobnie rzecz się ma z newralgicznymi komputerami każdej sieci, czyli serwerami.

Najprostszym złamaniem niezbyt dobrych zabezpieczeń fizycznego dostępu jest przykład sprzątaczki. Sprzątacz czy sprzątaczka mają zazwyczaj bezproblemowy dostęp do wielu pomieszczeń, nikt nie zwraca raczej na nich uwagi, bowiem to normalne, że wszędzie mogą posprzątać jak również przekonanie o niedużym wykształceniu tych osób sprawia kamuflaż niemalże doskonały dla potencjalnego rabusia

danych. Trzeba pamiętać także, że zwykłe terminale podpięte do sieci od wewnątrz też są źródłem zagrożenia, gdy wpadną w niepowołane ręce, bowiem omijają wszelkie urządzenia zabezpieczające będące na styku świata zewnętrznego i naszej sieci.

Szczególnie na niezauważone ataki jesteśmy narażeni od wewnątrz w sieciach bezprzewodowych gdzie intruz nie ma de facto fizycznego kontaktu z siecią, a może się do niej dostać.

Powinniśmy także zdawać sobie sprawę z zagrożenia jakie mogą nieść dyski CD, dyskietki, dyski wymienne, na których mogą znajdować się niebezpieczne programy lub odwrotnie mogą znaleźć się dane prywatne, których tam nie powinno być.

Dopiero gdy podatności na fizyczne zagrożenia zostaną zminimalizowane możemy myśleć o sposobie zabezpieczeń na wyższych warstwach modelu odniesienia OSI. Gdy tego nie zrobimy nasze bezpieczeństwo pewnie runie jak dom ze złymi fundamentami.

Podsumowując ataki na system komputerowy ze względu na miejsce, z którego są przeprowadzane można podzielić na:

lokalne – intruz ma fizyczny dostęp do atakowanego komputera (są najgroźniejsze)

z sieci:

wewnętrzne – atak przeprowadzany z sieci, do której bezpośrednio włączony jest cel ataku

zewnętrzne (zdalne) – atakujący znajduje się w sieci zewnętrznej względem celu ataku (najtrudniejsze do przeprowadzenia i najbardziej widowiskowe)

Intruz atakuje nasz system komputerowy przeprowadzając serię ataków. Ataki te można podzielić na trzy grupy:

Ataki rozpoznawcze – zazwyczaj są pierwszym objawem próby włamania się. Polegają na zbieraniu informacji o uruchomionych komputerach, urządzeniach oraz uruchomionych na nich aplikacjach, systemie operacyjnym i jego wersji. Jest to tzw. rozpoznanie terenu, które nie jest szkodliwe oprócz zebranych informacji, które mogą być wykorzystane później.

Ataki dostępu – to już właściwy atak na uzyskanie konkretnych danych ich modyfikacji lub zniszczenia, bądź też uzyskaniu wysokich przywilejów w systemie operacyjnym. Ich szkodliwość jest bardzo duża.

Ataki blokowania usług (DoS – Denial of Service) – ma na celu uniemożliwienie właściwego korzystania z usług lub dostępu do sieci dla

autoryzowanych użytkowników. Jeżeli jest przeprowadzony z wielu komputerów naraz to nosi nazwę rozproszonego ataku blokowania usług (DDoS – Distributed Denial of Service). Nie jest aż tak niebezpieczny jak drugi typ ataku, ale szczególnie dla dużych korporacji może się taki stać i przynieść duże straty, ponieważ niedostępność usług świadczonych przez serwery firmy może zawieść zaufanie jej klientów i wpłynąć negatywnie na jej notowania.

Skutkiem ataku na system komputerowy może być:

Blokada tego systemu (atak z rodzaju DoS)

Przejęcie uprawnień autoryzowanego użytkownika systemu (przez co ma dostęp do informacji, które ten użytkownik może pozyskiwać, może zmienić ustawienia systemu, może wykorzystać system do dalszych ataków lub np. jako przekaźnik spamu tzw. open-proxy).

Dla potrzeb ochrony sieci komputerowej należy stworzyć właściwy system bezpieczeństwa. System bezpieczeństwa definiuje się, bowiem jako system teleinformatyczny osadzony w pewnym środowisku, w którym działa i zawiera w sobie pewien zbiór obiektów, które mają podatności, zbiór środków ochrony, zbiór podatności oraz zbiór zagrożeń, przed którymi chcemy się zabezpieczyć.

Źródło: http://cisco-ids-pix.eprace.edu.pl/621.Analiza_zagrozen_dla_sieci_komputerowej.html