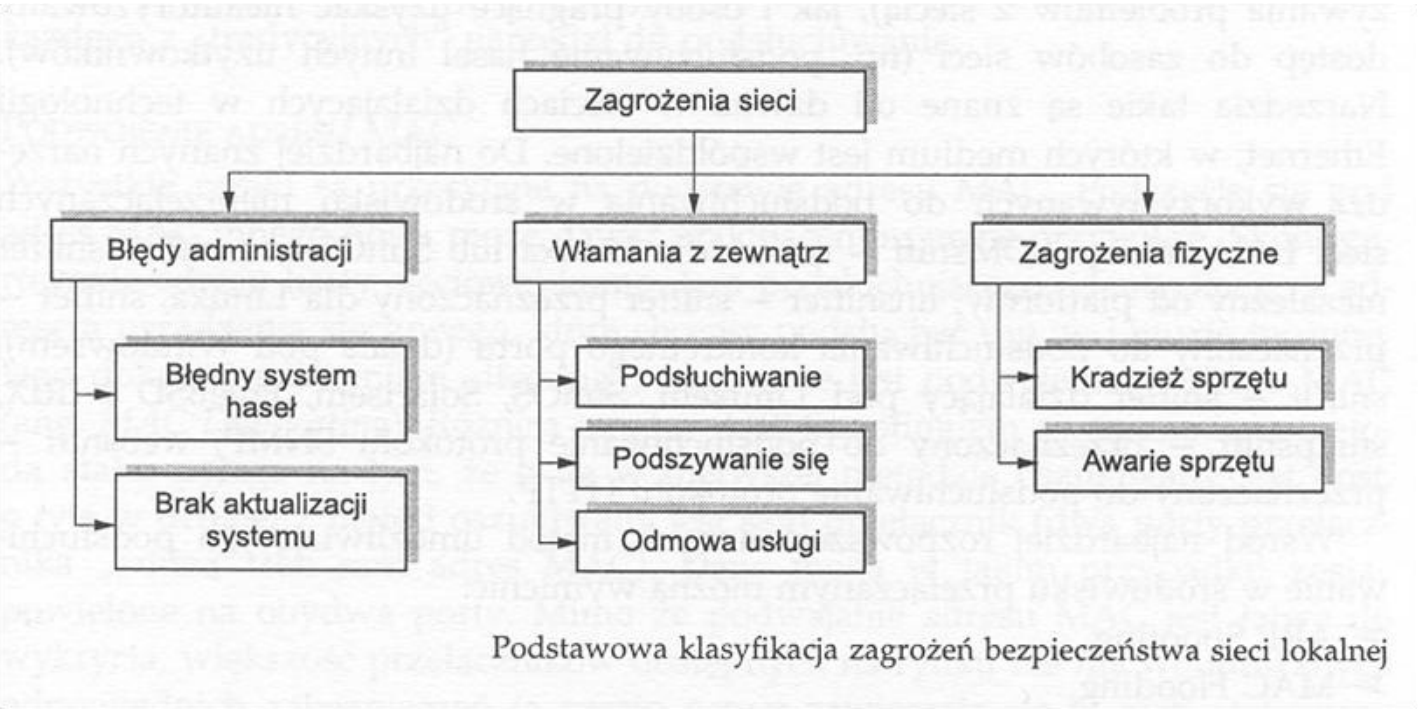
Rodzaje zagrożeń w sieciach.



Podstawowa klasyfikacja zagrożeń bezpieczeństwa sieci lokalnej

W nowym tysiącleciu nie trzeba już nikogo przekonywać, że nowoczesne technologie informatyczne są niezbędne dla rozwoju firmy. Obecnie oprócz tradycyjnych metod dotarcia do klienta (np. poprzez reklamę w mediach) bardzo ważnym staje się wizerunek firmy w Internecie. Niesie to za sobą także pewne niebezpieczeństwa.

Rodzaje zagrożeń sieci lokalnej z zewnątrz:

- Włamanie do komputerów sieci lokalnej w celu pozyskania haseł dostępu.
- Włamanie do serwera firmy i dostęp do bazy danych firmy (lista kontrahentów, przychody, plany rozwojowe, projekty firmy) Włamanie do sieci i zakłócenie jej pracy (każda godzina przestoju sieci przynosi firmie wymierne straty).
- Włamanie w celu uzyskania listy adresów e-mailowych firmy i jej kontrahentów w celu rozsyłania wirusów albo spamu poprzez pocztę elektroniczną.

Rodzaje zagrożeń sieci lokalnej od wewnątrz:

- Udostępnianie poprzez łącze internetowe poufnych danych przez pracownika firmy.

- Odwiedzanie serwisów WWW z zawartością nie związaną z działalnością firmy (strony rozrywkowe, pornograficzne, itp.).

- Ściąganie z Internetu różnego oprogramowania, które może zawierać wirusy lub destabilizować pracę komputera użytkownika. Używanie takiego oprogramowania nie musi być zagrożeniem dla pracy sieci, ale może być poprostu nielegalne.

Nie trzeba przekonywać nikogo, że ważne są zarówno zagrożenia napływające z zewnątrz (z Internetu) jak i od strony sieci lokalnej firmy. Aby przeciwstawić się tym zagrożeniom nie wystarczy już słowne lub pisemne poinformowanie pracowników o istniejących zagrożeniach.

Rozwiązaniem dla firm posiadających stały dostęp do Internetu jest Firewall (tzw. ściana ogniowa). Firewall jest to komputer, urządzenie łączące sieć lokalną firmy z siecią globalną (Internet). Zadaniem zapory Firewall jest zapobieganie nieautoryzowanym dostępom do sieci firmy z zewnątrz, a także ustalenie polityki bezpieczeństwa dla komputerów pracowników firmy. Polityka bezpieczeństwa w dużym stopniu ogranicza możliwość "zaszkodzenia" komputerom firmy przez ich pracowników. Zasada opiera się o przydzieleniu uprawnień dla każdego komputera co do dostępu do Internetu np. blokowanie portu SMTP do innych niż firmowego serwera.

Rozważmy przykład:

Firma "X" posiada pięć komputerów. Jeden to komputer Dyrektora, dwa kolejne to komputery sekretariatu i księgowości i dwa ostatnie to komputery działu sprzedaży. Firma zdecydowała się na stały dostęp do Internetu. W okresie silnego rozwoju firmy zatrudniony został nowy pracownik do działu sprzedaży, który korzystając z okazji podczas pracy intensywnie korzystał z zasobów Internetu. Podczas swoich wędrówek ściągnął nieświadomie do swojego komputera wirusa, który zainstalował się w systemie otwierając port 1234 w celu połączenia z innym komputerem sieci globalnej należącym np. do autora wirusa, który w ten sposób przegląda dysk zainfekowanej maszyny.

W takim przypadku luka w bezpieczeństwie sieci lokalnej firmy może zostać nie wykryta przez bardzo długi okres czasu. W tym czasie firma nieświadomie udostępniając swoje poufne dane może narazić się na wielkie straty.

Rozwiązaniem dla firmy "X" byłby Firewall, który blokowałby np. w okresie próbnym pracy nowego pracownika cały dostęp jego komputera do Internetu, natomiast po okresie próbnym zezwalałby na dostęp do wybranych usług internetowych i/lub wybranych serwisów WWW. Ze względu na szczególną poufność danych w księgowości Firewall zezwalałby tylko na połączenia szyfrowane z bankami. Na koniec ogólna polityka bezpieczeństwa zabraniałaby połączeń z niestandardowymi portami w sieci co skutecznie zablokuje działanie wszelkiego rodzaju wirusów otwierających "tylne drzwi" do sieci firmy. W takim przypadku nawet, gdy komputery firmy byłyby zainfekowane wyżej wspomnianym wirusem, a zainstalowane oprogramowanie antywirusowe nie wykryłoby nic, nie stanowiłoby to zagrożenia dla danych firmy.

Wniosek:

Skutecznie zastosowana zapora, nie tylko wspomaga lokalne systemy wykrywające zagrożenia (antywirusy, antyspamy, itp.), ale również pomaga w wykryciu potencjalnego zagrożenia poprzez rejestrację prób włamań (logi). Zmniejsza również skutki uboczne trwającego ataku (próby) od wewnątrz, przez to, że część ruchu jest ściśle wydzielona (dozwolony ruch tylko do zaufanych usług i serwerów).