STOSOWANIE METOD ZABEZPIECZANIA SPRZĘTU KOMPUTEROWEGO PRACUJĄCEGO W SIECI.

Zabezpieczenie współczesnych sieci teleinformatycznych wymaga kompleksowego podejścia i dokładnego zrozumienia tzw. słabych punktów sieci, które mogą narazić całą sieć, a w tym urządzenia sieciowe na wiele poważnych problemów włącznie z uszkodzeniem urządzenia. Szczegółowa wiedza dotycząca zabezpieczania sieci nigdy w pełni (w 100%) nie pozwoli zabezpieczyć sieci przed hakerami i ich próbami włamań, ataków itp.

Najsłabszym ogniwem występującym w sieci jest czynnik ludzki, który może w niekontrolowany, nieświadomy lub świadomy sposób uszkodzić urządzenia sieciowe oraz system operacyjny (rozpowszechniając wirusy).

Tylko całościowe i wszechstronne podejście do procesu zabezpieczenia sieci może zapewnić skuteczną ochronę urządzeń komputerowych pracujących w sieci. Budowanie sieci o wysokim stopniu skuteczności jest bardzo trudne w realizacji i bardzo kosztowne, dlatego też wiele firm decyduje się na tańsze i mniej skuteczne rozwiązania, ale zapewniające istotny poziom bezpieczeństwa sieci.

Najistotniejszym aspektem przy tworzeniu sieci jest określenie przedmiotu ochrony. Musimy dokładnie wiedzieć co chcemy chronić, gdyż tylko wtedy jesteśmy w stanie określić metody ochrony i zabezpieczeń.

Wszystkie elementy sieci powinny być dobrze udokumentowane, powinny być określone wartości tych elementów, tzn. każdy z elementów sieci powinien mieć przypisane jakieś znaczenie.

W każdej dobrze zabezpieczonej sieci muszą wystąpić takie elementy jak: serwery, stacje robocze, pamięci masowy (w tym całe systemy pamięci masowych), routery, przełączniki, koncentratory, łącza teleinformatyczne, zasilacze awaryjne (UPS), drukarki.

Bezwzględnie należy określić mogące wystąpić zagrożenia, zarówno te zewnętrzne (wirusy sieciowe, wiadomości email z wirusami, ataki zewnętrzne, zagrożenia energetyczne - wyładowania atmosferyczne, skoki napięcia w zewnętrznej sieci energetycznej, itp.), jak i wewnętrzne (przeglądanie zewnętrznych witryn w sieci Internet, wirusy rozprowadzane przez użytkowników sieci poprzez nośniki danych, wewnętrzne zakłócenia zasilania, fizyczne uszkodzenia sprzętu, itp.).

Przy tworzeniu sieci komputerowej należy kierować się zasadami pozwalającymi na zabezpieczenie sprzętu komputerowego zgodnie z założeniami. Należy tu wziąć pod uwagę środowisko, w jakim system komputerowy będzie pracował.

Sposoby i i metody zabezpieczania systemów komputerowych oraz systemów operacyjnych przed nieautoryzowanym dostępem zostaną

omówione w ramach tematu o zabezpieczaniu systemu operacyjnego. Tutaj skupimy się na zabezpieczeniach przed atakami, przed uszkodzeniami z powodów energetycznych itp.

Ochrona sieci przed naruszeniami bezpieczeństwa.
Sieci są szczególnie wrażliwe na naruszenia bezpieczeństwa i ataki, zarówno na szkielet sieci, jak i poszczególnie hosty. Atak może pochodzić zarówno z zewnątrz, jak i z wnętrza sieci. Często wysiłki administratorów skupiają się na zabezpieczeniu sieci lokalnej od strony Internetu, pomijany jest natomiast aspekt zabezpieczeń przed intruzami z własnej sieci.
Ochrona sieci nie powinna skupiać się wyłącznie na zagrożeniach czysto sieciowych i programowych. Należy pamiętać o tak prozaicznych zagadnieniach jak zabezpieczenie infrastruktury przed fizycznym wtargnięciem czy odpowiednia edukacja użytkowników na każdym poziomie.

Edukacja użytkowników sieci.
Edukacja użytkowników jest bardzo ważnym elementem polityki bezpieczeństwa. Ludzie są podatni na tzw. inżynierię społeczną (ang. social engineering), czyli techniki manipulacji ze strony innych osób. Człowiek okazuje się być często najsłabszym ogniwem systemu komputerowego. Zabezpieczenie sieci za pomocą wymyślnych urządzeń, list kontroli dostępu, firewalli może okazać się nic nie warte, jeśli napastnikowi uda się zdobyć zaufanie osób mających dostęp do sieci. Intruz może „zmieniać skórę” zależnie od sytuacji i od tego, z kim aktualnie rozmawia. Oczywiście im lepiej uświadomiony użytkownik, tym mniejsza szansa napastnika na zdobycie interesujących go informacji. W sieciach korporacyjnych edukację użytkowników należy przeprowadzać począwszy od pracowników najniższego szczebla, poprzez „zwykłych” użytkowników, na administratorach sieci i kadrze kierowniczej kończąc.

Zapory ogniowe.
Firewall zwany również zaporą lub ścianą ogniową jest jednym z najpopularniejszych i najskuteczniejszych sposobów ochrony sieci przed atakami i nieautoryzowanym dostępem. Jego rolą jest oddzielenie sieci zaufanej od niezaufanej, np. firmowej sieci lokalnej od Internetu lub wewnętrznej sieci firmowej od tzw. strefy zdemilitaryzowanej (DMZ), w której uruchomione są usługi dostępne dla klientów (np. serwer WWW z informacjami o przedsiębiorstwie). Zapora może chronić zarówno całą sieć (wtedy będzie uruchomiona na routerze lub moście sieciowym), jak i pojedyńcze hosty, np. szczególnie ważne serwery.

Filtracja pakietów.
Ochronę sieci za pomocą firewalli realizuje się na różne sposoby. Jednym z nich jest filtrowanie pakietów, polegające na analizie pakietów

sieciowych przechodzących przez zaporę w obu kierunkach i przepuszczania tylko dozwolonego ruchu. Analiza jest przeprowadzana zazwyczaj na podstawie protokołu komunikacyjnego i/lub portu, na jakim nadaje/nasłuchuje dana usługa. Filtrowanie pakietów jest realizowane programowo (np. za pomocą programu iptables dostępnego w Linuksie, pf w systemie OpenBSD lub ipfw z systemu FreeBSD) bądź na dedykowanych urządzeniach, które oprócz filtrowania i kontroli poprawności pakietów mogą wykonywać również inne zadania (np. ochronę antywirusową czy odsiewanie spamu).

Serwery pośredniczące (proxy).
Innym środkiem ochrony sieci jest stosowanie serwerów pośredniczących (proxy). Ich działanie polega na tym, że użytkownik chcący uzyskać dostęp do pewnego zasobu lub usługi najpierw łączy się z pośrednikiem, który w imieniu użytkownika łączy się ze zdalnym hostem i dopiero wtedy udostępnia żądany zasób użytkownikowi. Ma to tę zaletę, że użytkownik może dostać zawartość odfiltrowaną według reguł zdefiniowanych przez administratora proxy (tzw. content filtering). Serwery proxy są zazwyczaj kojarzone z przyspieszaniem ładowania stron WWW poprzez magazynowanie w pamięci podręcznej elementów najczęściej pobieranych przez użytkowników. Mają również zdolność do ukrywania prawdziwego adresu IP użytkownika, podstawiając w jego miejsce adres IP serwera proxy.

Ochrona pojedynczych hostów.
Pojedyncze stanowiska komputerowe można chronić na wiele sposobów. Jednym z nich jest oczywiście firewall w postaci programu, często zintegrowany z ochroną antywirusową i antyspyware'ową. Prostym sposobem zapobiegania kradzieży wrażliwych danych lub uzyskania nieautoryzowanego dostępu do systemu operacyjnego przez intruza lub nieuczciwego pracownika jest uniemożliwienie korzystania z napędów wymiennych (stacji dysków, odtwarzaczy i nagrywarek płyt oraz pamięci flash) poprzez zablokowanie takiej możliwości na poziomie SO lub BIOS bądź przez zwyczajne wyjęcie napędu z obudowy.

Śledzenie zdarzeń.
Śledzenie i rejestrowanie zdarzeń zachodzących w systemie informatycznym są jednymi z najważniejszych zadań administracyjnych. Analiza dzienników systemowych (logów) pozwala na wychwycenie prób naruszenia bezpieczeństwa, daje informację o częstotliwości i powtarzalności tych prób, umożliwia stwierdzenie, czy próby te są przypadkowe i niezamierzone czy podejmowane z premedytacją i wymierzone w konkretny punkt systemu. Zapisy w logach pozwalają również na ustalenie źródeł ewentualnych ataków i prób naruszenia bezpieczeństwa. Niekiedy można na ich podstawie stwierdzić, jakich narzędzi używa intruz. W skrajnych przypadkach mogą stać się ważnym dowodem prawnym przeciwko napastnikowi.

STOSOWANIE METOD ZABEZPIECZANIA SPRZĘTU KOMPUTEROWEGO PRACUJĄCEGO W SIECI.

Wykrywanie ataków sieciowych.
Systemy wykrywania włamań (Intrusion Detection Systems, IDS) mają na celu wykrycie włamania lub innego naruszenia bezpieczeństwa i zebranie śladów tego zdarzenia do dalszej analizy lub jako dowód dla organów ścigania. Występują jako rozwiązania sieciowe (Network IDS, NIDS), składające się z czujników wykrywających zdarzenia, silnika zbierającego dane z czujników i generującego alarmy oraz konsoli administracyjnej wyświetlającej dane z czujników i alarmy bądź jako rozwiązania hostowe (Host IDS, HIDS), zabezpieczające pojedyncze systemy.

Systemy wykrywania włamań bazują na dwóch podstawowych metodach:
1. Wykrywanie w oparciu o sygnatury IDS sprawdza, czy ruch w sieci lub dostęp do systemu da się przypisać do znanych, ściśle określonych wzorców (sygnatur) będących oznakami ataku. Sygnaturą mogą być np. powtarzające się nieudane próby logowania.
2. Wykrywanie anomalii IDS sprawdza, czy sieć lub system informatyczny zachowuje się normalnie (trzeba zdefiniować „normalne zachowanie”!), np. czy poziom ruchu sieciowego nie wzrasta zbyt gwałtownie i bez uzasadnienia.

Plusy i minusy systemów IDS.
Zalety:
- wykrywanie ataków mających źródło poza siecią lokalną (NIDS) oraz wewnątrz LAN (HIDS)
- dobra skalowalność (szczególnie w przypadku NIDS)
- zarządzanie z centralnej konsoli
- mogą koegzystować z firewallami i pracować transparentnie
- mogą analizować dane na bieżąco i wstecz

Wady:
- nie powstrzymują ataków, tylko je rejestrują
- mogą generować fałszywe trafienia (false positives) i usypiać czujność
- lub pomijać pewne typy ataków
- muszą być stale dostrajane (uzupełnianie sygnatur ataków)
- w szybkich i rozległych sieciach mogą powodować opóźnienia

Zapobieganie atakom sieciowym.

Systemy wykrywania włamań są z definicji pasywne – pomagają w stwierdzeniu samego faktu włamania, ale nie potrafią zapobiegać atakom w trakcie ich trwania. Tę niedogodność usuwają systemy zapobiegania włamaniom (Intrusion Prevention Systems, IPS) – są rozwiązaniami aktywnymi, dynamicznie reagującymi na naruszenia bezpieczeństwa. Sieciowy IPS to w praktyce NIDS z analizą ruchu inline (tzn. bezpośrednio na łączu sieciowym) i możliwością dynamicznego podejmowania określonych działań w odpowiedzi na wykryty atak (np. modyfikacja danych w warstwie aplikacji lub zmiana reguł list dostępu). Hostowy IPS to HIDS sprzężony z firewallem aplikacyjnym (proxy). IPS potrafią działać na poziomie aplikacji (warstwa 7 modelu OSI), czyli analizować protokoły przeznaczone dla konkretnych aplikacji (np. HTTP, SMTP, FTP).

Pułapki na intruzów.

Oprócz wykrywania włamań i zapobieganiu im nie jesteśmy ograniczeni tylko do bycia ofiarą. Stosunkowo łatwo możemy zamienić się rolami z napastnikiem. Podglądanie jego działań i wysiłków oraz analiza używanych technik i narzędzi daje nam pojęcie o poziomie umiejętności intruza, a często informuje o jego zamiarach (zabawa, chęć sprawdzenia się, próba kradzieży danych, próba przejęcia sieci. . .). Zwabienie włamywacza w pułapkę daje nam również cenny czas na ewentualne wprowadzenie dodatkowych zabezpieczeń na poziomie sieci lub pojedynczych hostów. Rozwiązania mające na celu zwabienie potencjalnego intruza w pułapkę określa się nazwą honeypot (garnek miodu) lub po prostu przynętą.