**TEMAT: Metody zabezpieczania systemów komputerowych – Zapory sieciowe**

Temat obejmuje 2 godziny lekcyjne

Bezpieczeństwo systemów informatycznych może być rozpatrywane w trzech aspektach: poufność (ang. confidentiality), integralność (ang. integrity) oraz dostępność (ang. availability). Poufność definiowana jest jako zabezpieczenie lub ukrycie informacji przed niepowołanym dostępem. Integralność odnosi się zazwyczaj do zabezpieczania danych przed niepowołaną modyfikacją, tak aby użytkownik miał zaufanie do informacji i źródła jej pochodzenia. Dostępność natomiast oznacza możliwość używania pożądanych zasobów zgodnie z ich przeznaczeniem

Analizując dotychczas znane mechanizmy zabezpieczania systemów komputerowych można wyróżnić trzy grupy. Do pierwszej należy zaliczyć mechanizmy filtrowania ruchu sieciowego, które pozwalają na blokowanie zdalnego dostępu do sieci lokalnych i komputerów. Tego typu mechanizmy mają szerokie zastosowanie z uwagi na duży udział włamań do systemów komputerowych poprzez sieć Internet. Do drugiej grupy należą mechanizmy pozwalające na ograniczanie szkód jakich może dokonać intruz po udanym włamaniu do systemu. Tego typu mechanizmy mają bardzo duży potencjał i dlatego są rozwijane w wielu ośrodkach naukowo-badawczych na całym świecie. W trzeciej grupie mechanizmów zabezpieczania można umieścić metody pozwalające na wykrywanie włamań oraz kontrolę plików pod kątem ich nieuprawnionych modyfikacji przez intruzów.

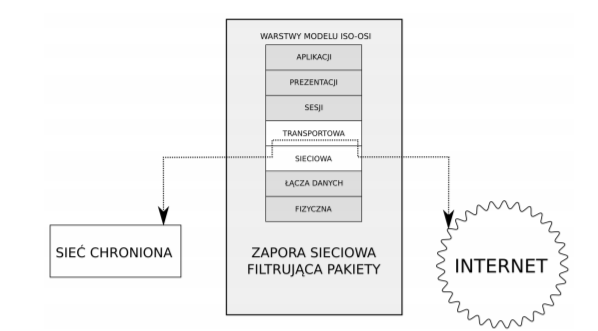
W tabeli przedstawiono pokrycie aspektów bezpieczeństwa przez systemy wchodzące w zdefiniowane wyżej grupy mechanizmów. Dodatkowo, z grupy systemów wykrywania włamań zostały wyodrębnione systemy ochrony integralności plików, a z mechanizmów ograniczania skutków włamań, wirtualizacja.



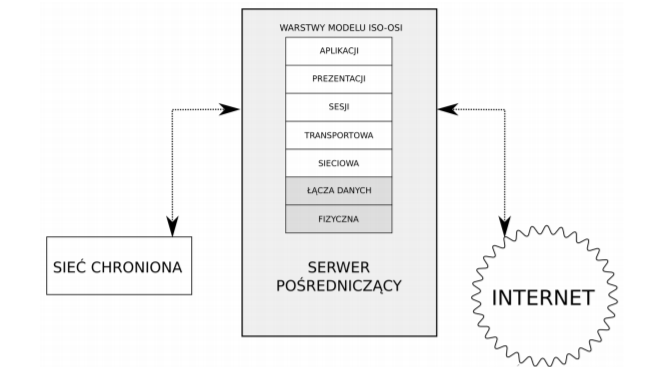
Mechanizmy filtrowanie ruchu sieciowego Bardzo skutecznym sposobem zapewnienia bezpieczeństwa systemu komputerowego jest całkowite odizolowanie go od sieci Internet. Taka praktyka jest z powodzeniem stosowana w wielu instytucjach np. finansowych i wojskowych. Pomimo oczywistych wad takiego rozwiązania i zmniejszenia funkcjonalności systemu, w pewnych przypadkach takie działania są sensowne i całkowicie uzasadnione. Obecnie tylko niewielka część komputerów działa w ten sposób. Zdecydowana większość maszyn jest podłączona do sieci globalnej. Dotyczy do zarówno komputerów domowych, firmowych czy np. serwerów obliczeniowych. Zamiast całkowitego odłączenia komputera od sieci Internet powszechnie stosuje się rozwiązanie mniej restrykcyjne, choć podobne w swoim działaniu. Filtruje się ruch sieciowy wychodzący i przychodzący do systemu komputerowego według określonych zasad. Narzędzia służące do tego celu noszą nazwę zapór sieciowych (ang. firewall). Zapora sieciowa jest to system lub grupa systemów, które kontrolują ruch pomiędzy dwoma sieciami komputerowymi i na podstawie zdefiniowanych reguł przepuszczają lub blokują połączenia. W ten sposób systemy komputerowe chronione są przed niepowołanym dostępem do zasobów .

Zabezpieczenie typu firewall pozwala na filtrowanie ruchu sieciowego pomiędzy siecią globalną i lokalną. W ten sposób można ograniczyć dostęp do zasobów lub usług tylko dla wybranej grupy komputerów działających poza siecią lokalną. Istnieje również możliwość kontroli dostępu do komputerów zewnętrznych przez użytkowników znajdujących się wewnątrz sieci. Zapory sieciowe są również skutecznym sposobem na ukrywanie architektury sieci lokalnych, pozwalają na autoryzowanie użytkowników, a także na śledzenie ruchu sieciowego.

Najpopularniejsza i zarazem najprostsza zapora sieciowa kontroluje ruch na podstawie danych zawartych w opisie pakietów sieciowych i jest nazywana zaporą sieciową filtrująca pakiety (ang. packet filtering firewall) . Jak pokazano na rysunku , zapory sieciowe tego typu kontrolują dane zapisane w warstwie sieciowej oraz transportowej modelu ISO-OSI. Pozwala to na filtrowanie pakietów pochodzących z określonych adresów IP, wyróżnionych sieci lub podsieci, czy też konkretnych portów TCP lub UDP. Tego rodzaju zapory pozwalają np. na udostępnianie usług działających na wskazanych portach tylko ściśle określonym komputerom. Umożliwiają również całkowite zablokowanie ruchu sieciowego pochodzącego z komputera znajdującego się w określonej podsieci



Innym typem zapory sieciowej jest tzw. serwer pośredniczący (ang. proxy server), który działa na najwyższej warstwie modelu OSI, warstwie aplikacji. Jego działanie polega na całkowitym odseparowaniu chronionej sieci lokalnej od Internetu. W rezultacie komputer w sieci wewnętrznej nie może nawiązać bezpośredniego połączenia z żadnym zewnętrznym serwerem. Wszelki kontakt dokonywany jest poprzez serwer proxy, który nawiązuje połączenie z komputerem docelowym.



W ten sposób połączenie klient-serwer jest całkowicie kontrolowane poprzez zaporę pośredniczącą co daje administratorom większą kontrolę nad ruchem sieciowym, można np. kontrolować połączenia wykonywane przez aplikacje. Można powiedzieć, że serwer pośredniczący jest umieszczony na pierwszej linii ataku, jednak w związku z tym, że nie działają na nim żadne aplikacje, ani nie są przechowywane ważne dane, straty wynikające z udanego włamania lub jego zniszczenia są stosunkowo niskie. Uszkodzenie serwera proxy nie powoduje automatycznego uszkodzenia żadnych zasobów komputerowych znajdujących się w sieci lokalnej, co mogłoby się przekładać na znaczące straty dla użytkowników

W celu zwiększenia skuteczności zapór sieciowych stosuje się połączenie różnych metod i mechanizmów filtrowania pakietów. Jednak należy stwierdzić, że nawet najbardziej złożone zapory sieciowe nie są w stanie całkowicie ochronić systemu komputerowego. Pozwalają jedynie na częściowe lub całkowite odseparowanie sieci lokalnej od środowiska zewnętrznego.

Zapory sieciowe nie chronią przede wszystkim przed następującymi zagrożeniami:

* wirusami komputerowymi,
* końmi trojańskimi,
* atakami dokonywanymi wewnątrz sieci lokalnej,
* atakami wykorzystującymi błędy w aplikacjach.