Sieci komputerowe i programowanie sieciowe

7. Zasady budowy i wykorzystania zapór sieciowych w różnych warstwach modelu OSI

Zapora sieciowa (firewall) - jest to jeden ze sposobów zabezpieczenia sieci i systemów przed intruzami.
Termin ten może się odnosić zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, na którego straży stoi. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrzenj LAN przed dostępem z zewnątrz, tzn sieci publicznej, internetu. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odnawianie żądań dostępu uznanym za niebezpieczne.
Najczęściej używanymi technikami obrony sa:

- filtrowanie pakietów, czyli sprawdzanie pochodzenia pakietów i akceptowanie pożądanych,
- stosowanie algorytmów identyfikacji użytkownika (hasła, cyfrowe certyfikaty),
- zabezpieczanie programów obsługujących niektóre protokoły (np. FTP)

Bardzo ważną funkcją zapory sieciowej jest monitorowanie ruchu sieciowego i zapisywanie najważniejszych zdarzeń do dziennika (logu). Umożliwia to administratorowi wczesne dokonywanie zmian konfiguracji. Poprawnie skonfigurowana zapora powinna odeprzeć wszelkie znane typy ataków. Na zaporze można zdefiniować strefę ograniczonego zaufania – podsieć, która izoluje od wewnętrznej sieci lokalne serwery udostępniające usługi na zewnątrz.

Typy zapór sieciowych

- Zapory filtrujące – monitorują przepływające przez nie pakiety sieciowe i przepuszczają tylko zgodne z regułami ustanowionymi na danej zaporze (zapora pracująca dodatkowo jako router). Zwykle w niewielkich sieciach jest zapora sprzętowa bądź wydzielony komputer z systemem operacyjnym Linux. Obecnie najczęściej wykorzystywana metoda filtrowania w Linuksie to reguły oparte na iptables. Dostępne są także zamknięte komercyjne rozwiązania programowe, z których wiele posiada bardzo wymyślne własności i rozbudowany system konfiguracji oraz wiele możliwych do zintegrowania rozwiązań, pozwalających nie tylko na analizę i filtrowanie pakietów IP, ale także na sprawdzanie poprawności pakietów z punktu widzenia wyższych warstw modelu ISO/OSI, a nawet na prowadzenie ochrony antywirusowej.
- Translacja adresów sieciowych (ang. *network address translation*, NAT) – polega na dokonywaniu zmiany adresu IP hosta wewnętrznego w celu ukrycia go przed zewnętrznym monitorowaniem. Mechanizm ten jest również nazywany maskowaniem adresu IP.

- Zapory pośredniczące (*proxy*) – wykonujące połączenie z serwerem w imieniu użytkownika. Przykładowo, zamiast uruchomienia sesji http bezpośrednio do zdalnego serwera WWW, uruchamiana jest sesja z zaporą i dopiero stamtąd uruchamiane jest połączenie z systemem zdalnym. Cała komunikacja na serwer http przechodzi przez serwer pośredniczący (*proxy*), które może filtrować ruch. *Proxy*, jeśli ma taką funkcjonalność, potrafi rozpoznać komendy http, jak i analizować zawartość pobieranych stron WWW (działa w warstwie aplikacji modelu ISO/OSI). Zabezpieczające działanie zapory, z punktu widzenia klienta, polega w tym wypadku na tym, iż możliwe jest zablokowanie wybranej treści (ang. *content filtering*), aby nie dotarła ona do klienta (np. strony ze słowami wulgarnymi, o treści pornograficznej itp.).

Współcześnie często pracująca zapora sieciowa jest rozwiązaniem hybrydowym analizującym pakiety od warstwy łącza danych do aplikacji modelu OSI. Umożliwia realizację złożonych polityk bezpieczeństwa oraz integrację z systemami IDS. Skuteczna ochrona zasobów IT oznacza całościowe działania, kierujące ku podstawom bezpieczeństwa. Najważniejsze jego elementy dotyczą infrastruktury, backupu, danych osobowych, zabezpieczenia przed problemami wynikającymi z utraty zasilania czy chociażby awarii chłodzenia.