

Ściany ogniowe

Wykrywanie intruzów

ŚCIANY OGNIOWE

1. Zagrożenia płynące z Internetu

Bezpieczeństwo to zagadnienie istotne zarówno dla firm jak i dla indywidualnych użytkowników. Internet to znakomite narzędzie zarówno do dystrybucji informacji o sobie jak i otrzymywaniu ich od innych, jednak z wszelkimi dobrodziejstwami globalnej sieci związana jest również pokaźna liczba zagrożeń. Przestępstwa komputerowe takie jak kradzież informacji czy celowe niszczenie danych to tylko niektóre z nich.

Najlepszym sposobem uniknięcia takiego biegu wydarzeń jest podjęcie działań prewencyjnych związanych z pozbawieniem możliwości uzyskania dostępu przez sieć do maszyny. To pole zastosowań dla firewalli (ścian ogniowych, zapór ogniowych).

1.1. Metody ataków

Ogólnie metody włamań możemy podzielić na:

- ataki z zewnątrz sieci lokalnej
- ataki z wnętrza sieci lokalnej
- ataki pośrednie

1.1.1. Ataki z zewnątrz

Są to ataki, których najczęstszą formą są zakłócenia stabilnej pracy. Przejmowanie kontroli nad systemami odbywa się z zewnątrz sieci lokalnej na przykład z Internetu. Można w tym celu wykorzystać lukę w systemie zabezpieczeń, błąd serwisu sieciowego lub po prostu słaby poziom zabezpieczeń firmy. Do najczęstszych tego typu ataków należą:

- Ataki na poszczególne komputery bądź serwer główny (DoS, wirusy) – to jeden z najczęstszych typów ataków. Konsekwencjami są zwykle przerwy w pracy sieci lokalnej, uszkodzenie poszczególnych (bądź wszystkich) końcówek serwera, a co za tym idzie całej sieci, co powoduje wielogodzinne przerwy w pracy.

- Ataki na serwer http – to ataki, których efektem jest utrata danych witryny internetowej lub uzupełnienie jej treściami kompromitującymi firmę.

Do ataków z zewnątrz sieci hakerzy często wykorzystują metodę zwaną DoS. Jest to atak mający na celu zablokowanie konkretnego serwisu sieciowego (na przykład strony WWW) lub zawieszenie komputera. Możliwe jest przesterowanie ataków DoS do bardziej skomplikowanych metod, co może doprowadzić nawet do awarii całej sieci. Niejednokrotnie hakerzy, którzy włamują się do systemów za pomocą tzw. techniki spoofingu lub redykcji, ukrywają swój prawdziwy adres internetowy, więc ich zlokalizowanie często staje się niemożliwe. Anonimowość ułatwia więc zdecydowanie atakowanie systemów metodą Denial of Service (DoS), co powoduje uniemożliwienie wykonania przez serwer jakiegokolwiek usługi.

Spoofing (maskarada) – metoda ta stosowana jest zwykle przez doświadczonych i wyrafinowanych włamywaczy. Polega na podszyciu się włamywacza pod jednego z użytkowników systemu, który posiada własny numer IP (numer identyfikujący użytkownika). Technika ta ma na celu omijanie wszelkich zabezpieczeń, jakie zastosował administrator w sieci wewnętrznej. Jest bardzo skuteczna nawet, gdy bywa wykorzystywana przeciwko markowym firewallom, switchom i ruterom. Dzięki niej możliwe jest „udawanie” dowolnego użytkownika, a co za tym idzie „podszywanie” się i wysyłanie sfałszowanych informacji. Ze swego komputera haker może dokonać przekierowania źródłowego adresu IP i „podszyć się” pod komputer sieciowy. Robi to po to, by określić jego bezpośrednią drogę do miejsca przeznaczenia oraz trasę powrotną. W ten sposób może przechwytywać lub modyfikować transmisje bez zliczania pakietów przeznaczonych dla komputera głównego. W przeciwieństwie do ataków polegających na rozsynchrozowaniu, „podszywanie się” pod adresy IP jest trudne do wykrycia. Jeśli serwer internetowy ma możliwość monitorowania ruchu w sieci w zewnętrznym routerze internetowym, to należy kontrolować przechodzące przez niego dane. Do sieci nie powinny być wpuszczane pakiety zawierające adresy komputera źródłowego i docelowego, które mieszczą się w obrębie lokalnej domeny. Najlepszą obroną przed podszywaniem się jest

filtrowanie pakietów wchodzących przez ruter z Internetu i blokowanie tych, których dane wskazują na to, że powstały w obrębie lokalnej domeny.

1.1.2. Ataki z wnętrza sieci

Ataki z wnętrza sieci należą do jednych z groźniejszych. Włamanie następuje z wnętrza sieci lokalnej poprzez wykorzystanie konta jakiegoś użytkownika czy też luki w zabezpieczeniach systemu autoryzacji użytkowników. Najczęściej włamania tego typu są udziałem pracowników firmy, a nie użytkowników komputerów spoza jej obrębu, gdyż dostęp do końcówki Sieci takiej osoby rzadko pozostaje zauważony.

1.1.3. Ataki pośrednie.

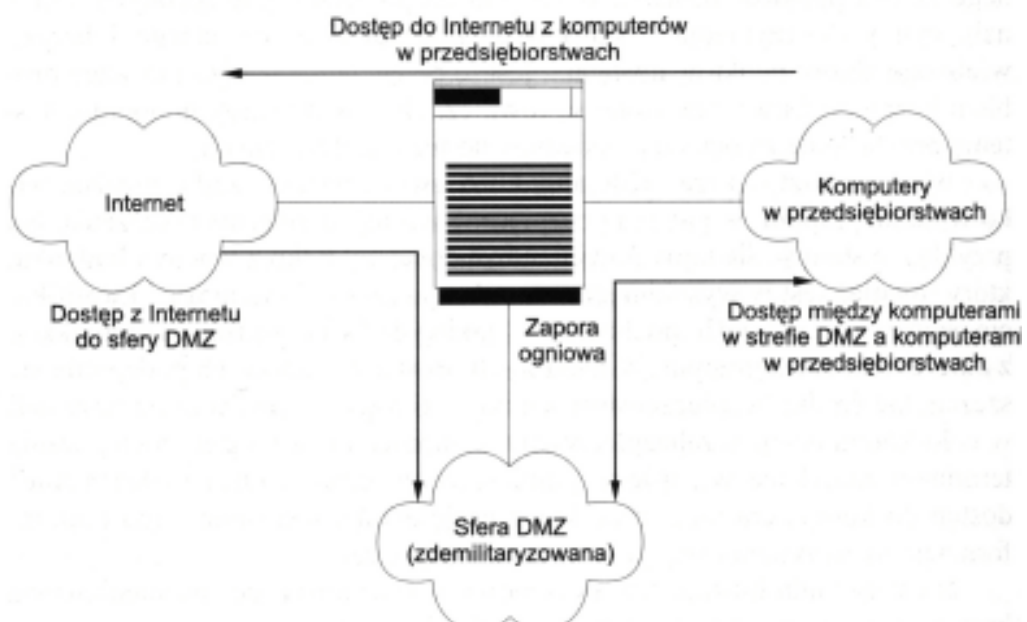
Hakerzy stosują tu dość wyrafinowane metody, czego najlepszym przykładem są konie trojańskie. To grupa ataków najtrudniejszych do wykrycia. „Podłożenie” konia trojańskiego otwierającego dostęp do całej sieci może odbyć się za pośrednictwem poczty elektronicznej czy też podczas ściągania programu, który pochodzi z niepewnego źródła. Użytkownik prawie nigdy nie jest świadom tego, że ściągając na przykład najnowszą wersję odtwarzacza plików mp3 faktycznie otwiera dostęp do swojego komputera, a potem całej Sieci osobom niepowołanym.

Packet sniffing (podsluchiwanie pakietów) jest to metoda zdobywania systemu polegająca na przechowywaniu przesyłanych przez sieć niezaszyfrowanych informacji. Można w ten sposób zdobyć hasło użytkownika i uzyskać dostęp do danego konta. Ataki polegające na „biernym węszeniu” stały się powszechne w Internecie. Stanowią one zazwyczaj wstęp do aktywnego przechwytywania cudzych plików. Aby rozpocząć tego rodzaju atak, haker musi zdobyć identyfikator i hasło legalnego użytkownika, a następnie zalogować się do Sieci. Kiedy wykona już te posunięcia, może bezkarnie podglądać i kopiować transmisje pakietów, zdobywając jednocześnie informacje o funkcjonowaniu danej sieci lokalnej.

Ataki korzystające z autoryzowanego dostępu są to ataki często stosowane przez osoby próbujące się włamać do sieci opartych na systemie operacyjnym (takim jak UNIX, VMS i Windows NT), korzystającym z mechanizmu autoryzowanego dostępu. Duże niebezpieczeństwo niesie ze sobą tworzenie plików zawierających nazwy serwerów, do których można uzyskać dostęp bez podawania hasła.

2. Zabezpieczenie za pomocą firewalla

Pojawił się problem zabezpieczenia prywatnych sieci przed nieautoryzowanym dostępem z zewnątrz. Administrator musi oddzielić lokalną sieć od internetowego chaosu, żeby dane nie dostały się w niepowołane ręce lub nie zostały zmienione.



Rys.: Wydzielenie domen odseparowanych zaporą ogniową

Źródło: Silberschatz A., Galvin P.: (2002). Podstawy systemów operacyjnych. Warszawa: WNT, strona: 754

Firewall może zabezpieczyć sieć przed nieuprawnionym dostępem z zewnątrz. Zakres dostępnych rozwiązań sięga od dodatkowego oprogramowania do specjalnych urządzeń, które służą tylko do tego celu.

3. Czym jest firewall?

Firewall składa się z pewnej liczby komponentów sieciowych (sprzętowych i programowych) w punkcie styku dwóch sieci. Zapewnia zachowanie reguł bezpieczeństwa między siecią prywatną a niezabezpieczoną siecią publiczną, na przykład Internetem.

Właśnie ta zaporę decyduje, które z usług w sieci prywatnej dostępne są z zewnątrz i z jakich usług niezabezpieczonej sieci publicznej można korzystać z poziomu sieci prywatnej. Aby firewall był skuteczny, cały ruch danych między siecią prywatną a Internetem musi przechodzić przez niego.

Firewall nie jest, jak router, bastion host czy inne urządzenie, częścią sieci. Jest jedynie komponentem logicznym, który oddziela sieć prywatną od publicznej. Bez firewalla każdy host w sieci prywatnej byłby całkowicie bezbronny wobec ataków z zewnątrz.

4. Funkcje firewalla

Firewall spełnia wiele funkcji, których zakres może obejmować:

4.1. Kontrolę dostępu do usług systemu

Kontrola jest prowadzona w stosunku do użytkowników zewnętrznych oraz tych pracowników firmy, którzy z pewnych przyczyn przebywają tymczasowo poza terenem organizacji i muszą korzystać z usług systemu. Niekiedy zezwala się także, aby pracownicy dokonywali zdalnych połączeń z systemem informatycznym organizacji za pośrednictwem sieci Internet, pracując na swoich komputerach domowych. Ściana ogniowa po zidentyfikowaniu użytkownika dokonuje uwierzytelnienia jego tożsamości, czyli sprawdzenia, czy jest tym, za kogo się podaje.

Uwierzytelnienie może się odbywać zgodnie z wybraną metodą:

- hasło (wielokrotnego użytku, jednorazowe)
- karty magnetyczne lub mikroprocesorowe
- systemy biometryczne

4.2. Ograniczenie liczby dostępnych usług

Ograniczanie usług odnosi się do blokowania serwerów funkcjonujących zarówno w sieci prywatnej, jak i w Internecie. Myśląc o bezpieczeństwie systemu informatycznego należy ograniczyć dostępność określonych usług dla użytkowników zewnętrznych. Również ze względów bezpieczeństwa oraz niekiedy w celu zmniejszenia kosztów można zablokować pewne usługi dla pracowników lokalnych.

4.3. Kontrolowanie połączeń sieciowych

Kontrolowanie odbywa się w niższych warstwach modelu OSI i dzięki temu może być przezroczyste dla użytkowników i aplikacji. Następuje przechwytywanie pakietów danych i sprawdzanie czy rozpoznane połączenie sieciowe jest dozwolone. Ściana ogniowa akceptuje lub blokuje próby zainicjowania komunikacji sieciowej między określonymi komputerami. W dużych sieciach korporacyjnych często przyjmuje się konfigurację, w której komputery mogą prowadzić komunikację wyłącznie w środowisku sieci prywatnej.

4.4. Skanowanie serwisów sieciowych

Skanowanie serwisów sieciowych jest najczęściej prowadzone w stosunku do popularnych usług internetowych: WWW, FTP i poczty elektronicznej. Ściana ogniowa nadzoruje sposób i charakter wykorzystania tych usług, na podstawie pewnych przyjętych reguł ochrony oraz ustaleń organizacyjnych. Można na przykład określić, o której godzinie, w których dniach tygodnia i za pośrednictwem jakich komputerów pracownicy firmy mogą korzystać z zasobów odpowiednich serwerów WWW i FTP. W odniesieniu do poczty elektronicznej można wyobrazić sobie sytuację, w której firewall skanuje wszystkie nadchodzące i wychodzące przesyłki pocztowe oraz poddaje je określonej obróbce, np. usunięciu pewnych typów załączników, zmianie adresu nadawcy lub odbiorcy.

4.5. Wykrywanie i eliminowanie prób włamania do systemu

Wykrywanie i eliminowanie prób włamania do systemu jest jednym z najważniejszych zadań stawianych systemowi ściany ogniowej, od którego w dużej mierze zależy bezpieczeństwo całej organizacji. Firewall powinien być przygotowany do odparcia ataków typu „spoofing”, „source routing”, „source porting”, „SYN Flood”, „Ping of Death” oraz wszystkich innych znanych technik stosowanych przez hackerów.

4.6. Zabezpieczenie przesyłanych informacji

Ochrona danych przesyłanych w sieci publicznej sprowadza się do tworzenia wirtualnych sieci prywatnych. Jest to sieć logicznych kanałów transmisji danych, tworzonych na bazie sieci publicznej, otwieranych (najczęściej) na czas transferu danych między stacjami ścian ogniowych sieci prywatnych, poprzez które odbywa się przesyłanie informacji w formie zaszyfrowanej. Niektóre rozwiązania pozwalają także na tworzenie sieci VPN (ang. Virtual Private Network) między ścianą ogniową a odległymi komputerami użytkowników.

4.7. Nadzorowanie pracy routerów

Nadzorowanie pracy routerów jest konieczne w przypadku dużych sieci komputerowych, gdzie stosowanie jednego routera dostępu nie jest wystarczające. Takie sieci są wyjątkowo narażone na ataki hackerów, ponieważ istnieje wiele dróg wejścia do systemu i można łatwiej obejść jego zabezpieczenia. Routery mogą z powodzeniem zostać włączone do ściany ogniowej jako „przednia straż” prywatnej sieci komputerowej. Router może prowadzić filtrowanie pakietów danych, szyfrowanie i uwierzytelnianie przesyłanych informacji, a także przeciwdziałać włamaniom typu „Spoofing”.

4.8. Ochronę systemu przed niebezpiecznymi programami

Ochrona systemu odnosi się głównie do najnowszych rozszerzeń możliwości serwisu informacyjnego WWW. W ramach strony HTML można uruchamiać programy Java,

JavaScript, VisualBasic Script oraz ActiveX. Obecnie tylko technologia Java ma na tyle mocne mechanizmy zabezpieczeń, że można ją wykorzystywać bez obawy. Na inne rozszerzenia WWW można sobie pozwolić wówczas, gdy pochodzą z dobrze znanych i zaufanych serwerów. Współczesne ściany ogniowe potrafią sprawnie blokować dodatki do stron HTML, które pochodzą z określonych serwerów WWW.

4.9. Ukrywanie struktury wewnętrznej systemu

Ukrywanie struktury systemu ma na celu zmniejszenie ryzyka włamania z zewnątrz. Jest ono najczęściej realizowane przez tłumaczenie adresów komputerów sieci prywatnej. Technika tłumaczenia adresów sieciowych nosi nazwę NAT (ang. network address translation) i polega na odwzorowaniu wielu rzeczywistych adresów w jeden adres (widziany na zewnątrz sieci) lub bloku adresów w inny blok. Technicznie odbywa się to poprzez przechwytywanie pakietów danych i odpowiednią modyfikację zawartości ich nagłówek. Oprócz tłumaczenia adresów można wykonywać także translację numerów portów.

4.10. Monitorowanie bieżącego stanu komunikacji sieciowej

Monitorowanie bieżącego stanu komunikacji sieciowej umożliwia administratorowi wczesne zapobieganie określonym niekorzystnym zjawiskom np. włamaniom, dużemu obciążeniu routera itp. Na podstawie bieżącego stanu komunikacji, administrator może modyfikować parametry ściany ogniowej. Często stosowaną techniką jest blokowanie usług, a nawet całych stacji sieciowych (o niskim priorytecie), w celu zmniejszenia obciążenia systemu.

4.11. Rejestrowanie ważnych zdarzeń

Rejestrowanie zdarzeń umożliwia tworzenie raportów okresowych z działalności ściany ogniowej oraz pomaga w wykrywaniu sprawców łamania zasad przyjętej polityki ochrony systemu. Na podstawie analizy danych z archiwum, administrator może modyfikować konfigurację firewalla w celu wzmocnienia szczelności systemu ochrony.

4.12. Równoważenie obciążenia serwerów

Równoważenie obciążenia serwerów sieciowych jest uzasadnione w przypadku organizacji, które świadczą atrakcyjne usługi w sieci Internet. Pojedynczy serwer może wówczas być niewystarczający, a zastosowanie dodatkowych często kończy się sytuacją, w której jeden komputer jest nadmiernie obciążony, a inne pozostają bezczynne. Ściana ogniowa może przechwytywać zgłoszenia napływające od klientów z Internetu i kierować je do obsługi na wybrany serwer, zgodnie z pewnym przyjętym algorytmem rozdziału zadań.

Powyżej przedstawiono funkcje, jakie mogą pełnić firewalle. W funkcje te są wyposażone w mniejszym lub większym stopniu wszystkie ściany ogniowe dostępne na rynku.

Niestety nadmiar funkcji powoduje, że niedoświadczeni użytkownicy mają wielki problem z poprawnym skonfigurowaniem swoich zapór ogniowych. Wiele gazet poświęconych tematyce komputerowej zamieszcza artykuły, w których autorzy pomagają w konfiguracji.

Osoby, używające zapór: Sygate Personal Firewall 5.5, McAfee Firewall 4.02, Kerio Personal Firewall 4.0.13., odsyłam do artykułu pt.: „Za ścianą ognia” zamieszczonego w „CHIP” nr 5/2004 (strony: 134-138). Autorzy artykuły omówili dość szczegółowo podstawową konfigurację powyżej wymienionych ścian ogniowych.

5. Wady i ograniczenia zapór ogniowych

Firewall może tylko wtedy skutecznie chronić sieć, gdy wszystkie pakiety muszą przez niego przejść. Jeżeli na przykład w obrębie chronionej sieci zostanie ustanowione dodatkowe połączenie przez modem lub ISDN, użytkownicy mogą się łączyć bezpośrednio z Internetem przez PPP. Ci, którzy z jakichś powodów chcą uniknąć dodatkowego uwierzytelniania na serwerze proxy, szybko skorzystają z tej możliwości. Obchodząc firewall, stwarzają ogromne ryzyko ataku typu backdoor.

Firewall jest również bezużyteczny w wypadku ataku od wewnątrz. Nie zapobiegnie skopiowaniu poufnych danych na dyskietkę i wyniesieniu jej z firmy. Tym bardziej nie uniemożliwi działania pracownikowi, który ma duże uprawnienia lub ukradł hasła.

Firewalle nie ochronią też przed wirusami komputerowymi i trojanami, ponieważ nie sprawdzają każdego pakietu w poszukiwaniu szkodników. Nie radzą sobie także z **datadriven attacks**, polegających na wprowadzeniu pozornie niewinnych danych z ukrytym kodem, który może na przykład zmienić ustawienia zabezpieczeń.

Od dobrego firewalla należy oczekiwać, że będzie na tyle wydajny, żeby analiza danych nie spowalniała przepływu ich strumienia. Im szybsze łącze internetowe, tym więcej pakietów przepływa przez ścianę ogniową. Jeżeli ma ona również analizować strumienie danych – a więc nie tylko pakiety, ale także dane logiczne – potrzebny jest odpowiednio wydajny system.

Jak wyżej pokazano ściany ogniowe nie rozwiązują wszystkich problemów związanych z bezpieczeństwem. Należy pamiętać, że ściany ogniowe są tak dobre jak ich zasady. Niepełny zestaw nieodpowiednio określonych czy nawet nieodpowiednio obsługiwanych reguł może podważyć efektywność działania całej ściany ogniowej.

Zabezpieczenie systemu przez zaporę ogniową jest tak dobre jak ludzie, którzy ją programują i obsługują.

W przypadku każdego oprogramowania, które ma zabezpieczać system użytkownika – jak programy antywirusowe, zapory ogniowe itd. – okazuje się, że najsłabszym ogniwem jest sam użytkownik, któremu zależy na bezpieczeństwie. Wielu hackerów wykorzystuje właśnie ten fakt, o czym pisze w swojej książce Kevin Mitnick: „Sztuka podstępów” opublikowanej przez wydawnictwo Helion.

6. Przegląd rynku

Na rynku jest bardzo wiele zapór ogniowych, dlatego dość trudno jest dokonać wyboru. Nie zawsze okazuje się, że najdroższy produkt będzie najlepiej spełniał oczekiwania użytkownika i że będzie on „nie do przejścia”. Aplikacja pełniąca rolę ściany ogniowej, musi oprócz ataków z zewnątrz, radzić sobie atakami z wnętrza komputera. Hakerzy często tworzą programy, których zadaniem jest wyłączenie zapory, lub też zmiana ustawień.

Jednocześnie dobra zaporę powinna być dość prosta w obsłudze, aby poradził sobie z nią nawet początkujący. Z drugiej strony zaporę powinna oferować zaawansowane opcje konfiguracyjne, aby doświadczeni mogli precyzyjnie dostosować jej działanie do własnych potrzeb.

Przedstawię poniżej kilka zapór ogniowych (chyba najpopularniejszych) oraz opiszę zaporę, którą sam używam: Tiny Personal Firewall.

Zapory pogrupowałem według testu przeprowadzonego przez „PC World Komputer” („PC World Komputer, PRO”. Numer 2/2003. „Pora na zaporę”, strony: 112–118). Zapory występują w kolejności nieprzypadkowej. Jako charakterystykę przyjąłem stopień bezpieczeństwa, gdyż wydaje mi się, iż właśnie ten wskaźnik jest decydujący przy wyborze oprogramowania (najniżej na liście znajduje się zaporę, która uzyskała najgorszy rezultat).

- BlackICE Defender
- Look'n' Stop Lite
- Outpost Firewall Free
- Norman Personal Firewall
- Norton Personal Firewall PL
- Tiny Personal Firewall
- Deerfield Personal Firewall
- McAfee Firewall
- Sygate Personal Firewall
- Zone Alarm

Test przedstawiony przez gazetę jest dość miarodajny. Ukazuje jednocześnie, że jedne z lepszych zapór ogniowych są darmowe dla użytkowników prywatnych, natomiast za aplikacje, które wypadły w teście znacznie gorzej trzeba zapłacić.

7. Literatura

- 7.1. Forristal J., Traxler J.: (2003). Hack proofing. Your Web Applications. Gliwice: Helion.
- 7.2. Komar, B. (2002). TCP/IP dla każdego. Gliwice: Helion.
- 7.3. Niezgódka J.: (1998). Jak bronić się przed hackerami? Warszawa: Komputerowa Oficyna Wydawnicza „HELP”.
- 7.4. Silberschatz A., Galvin P.: (2002). Podstawy systemów operacyjnych. Warszawa: WNT.
- 7.5. Sportack M.: (1999). Sieci komputerowe. Księga eksperta. Gliwice: Helion.
- 7.6. Materiały z Akademii Górniczo-Hutniczej (P. Nowak, A. Majka, D. Kościelniak: Firewall).
- 7.7. „PC World Komputer PRO”. Nr 2/2003.
- 7.8. „PC World Komputer”. Nr 5/2004.
- 7.9. „CHIP”. Nr 3/2004.
- 7.10. „CHIP”. Nr 5/2004.