

Najnowsze trendy w dziedzinie zabezpieczeń sieci informatycznych. Firewalle aplikacyjne, IPS, IDS in-line

Wojciech Dworakowski

SecuRing

W ostatnich latach rozwinęły się nowe technologie związane ochroną zasobów w sieciach informatycznych. Okazało się, że tradycyjne technologie (firewall, IDS) nie są w stanie sprostać współczesnym zagrożeniom i sposobom ataku. Te nowe technologie, to m.in.:

- ¹ Firewalle aplikacyjne, które rozumieją ruch sieciowy chronionych aplikacji,
- ¹ IPS (Intrusion Protection System) – rozwinięcie technologii IDS o możliwość rozłączania podejrzanych połączeń sieciowych,
- ¹ IDS-inline – system wykrywania intruzów, który umie blokować próby włamań.

Technologie te do tej pory rozwijane w laboratoriach i jako open source najwyraźniej dojrzały już do wprowadzenia na rynek komercyjny. Widać to po najnowszych ofertach producentów systemów zabezpieczających.

Celem prezentacji będzie przybliżenie tych nowych technologii (a nie produktów!) również w kontekście chronienia zasobów udostępnianych przez instalacje Oracle i przygotowanie administratora na wybór właściwych rozwiązań.

Technologie omawiane podczas referatu zostaną dokładniej zaprezentowane podczas warsztatu „Zewnętrzne narzędzia zabezpieczające bazy danych i aplikacje przed włamaniami” (WP9 ataki)

Informacja o autorze:

Konsultant bezpieczeństwa IT w firmie SecuRing. Koordynator prac zespołu i osoba odpowiedzialna za sporządzanie raportów. Siedem lat doświadczenia praktycznego w zakresie bezpieczeństwa IT. Od trzech lat zajmuje się również testowaniem bezpieczeństwa produktów Oracle. Prelegent na licznych konferencjach poświęconych bezpieczeństwu IT (m.in. CERT Secure, PLOUG, Open Source Security, Windows Security). Prowadzi rubrykę poświęconą bezpieczeństwu w Biuletynie PLOUG.

Zabezpieczenia sieci teleinformatycznych to dziedzina rozwijająca się bardzo dynamicznie. Jej rozwój jest napędzany między innymi przez nowe badania i odkrycia w dziedzinie przeciwstawnej – atakowania systemów teleinformatycznych. Technologie ataku i zabezpieczeń prowadzą nieustanny wyścig. Na dodatek cały ten wyścig jest podsycany przez rozwój nowych technologii informatycznych. Szybko wprowadzane w życie nowe metody udostępniania i przetwarzania informacji, to zarówno wyzwanie dla atakujących jak i dla systemów zabezpieczających.

Technologie zabezpieczeń jeszcze kilka lat temu uważane za wystarczające, okazują się często bezsilne wobec nowych metod ataku. Wydaje się że rynek dojrzał już do zmian, widać to po ruchach producentów zabezpieczających. Niniejszy wykład ma na celu przybliżenie potencjalnym użytkownikom, kilku technologii jakie pojawiły się w ostatnim czasie lub będą wkrótce (zapewne agresywnie) wchodzić na rynek. Znajomość technologii stojących za poszczególnymi produktami pozwala na dokonanie racjonalnego wyboru popartego wnikliwą analizą przydatności a nie tylko opartego na zapewnieniach producentów.

Współcześnie eksploatowane systemy zabezpieczające przed atakiem zdalnym (z sieci)

Obecnie eksploatowane systemy zabezpieczające przed atakiem zdalnym z sieci zewnętrznej, to przede wszystkim firewalle i IDS-y (systemy wykrywania intruzów).

Firewalle klasy statefull inspection

Firewalle są technologią stosowaną w tej chwili powszechnie, nawet w najmniejszych firmach. W związku z powyższym nie będę szczegółowo omawiał zasad ich działania. Podstawowa funkcjonalność typowego firewalla to filtr pakietowy. Filtr taki posiada możliwość blokowania ruchu w zależności od parametrów takich jak:

- docelowy adres IP
- adres IP źródła
- port docelowy i port źródła
- protokół

Bardziej zaawansowane firewalle pozwalają filtrowanie biorące pod uwagę również inne parametry, jednakże filtry pakietowe nie wykraczają poza 4 warstwę protokołów OSI (TCP, UDP). W związku z tym, nie są w stanie odróżnić ataku przenoszonego przez protokoły wyższych warstw. Przykładem może być atak na aplikację obsługującą bankowość elektroniczną lub sklep internetowy. Dla firewalla taki atak będzie zwykłym ruchem HTTP.

W tej chwili na rynku dominują filtry klasy statefull inspection. Technika ta pozwala na analizę nie tylko pojedynczych pakietów, ale na kojarzenie pakietów w połączenia TCP (np. ściągnięcie strony WWW to przeważnie przesłanie kilkudziesięciu pakietów TCP). Dzięki temu że firewall „rozumie” takie pojęcie jak połączenie TCP, może on skuteczniej blokować próby przejścia firewalla oparte na manipulacji stanem w jakim znajduje się połączenie.

Konfiguracja firewalli opiera się na stworzeniu zestawu reguł wykorzystujących wyżej opisane parametry. Do każdej z reguł należy przypisać akcję jaką ma podjąć firewall. Typowo jest to:

- odrzucenie pakietu (atakujący zauważy, że pakiet został odrzucony)

- zignorowanie pakietu (atakujący nie otrzyma żadnej informacji)
- przepuszczenie pakietu.

Firewalle i Oracle

Większość protokołów stosowanych przez produkty Oracle nie ma większego problemu z integrowaniem się z firewallami. Wyjątkiem są te protokoły które nie działają na stałym porcie TCP lecz negocjują go w sposób dynamiczny. Pierwszy pakiet jest kierowany do pewnego stałego portu, przypisanego do usługi a potem jest negocjowany inny port na którym jest nawiązywana właściwa transmisja. Bywa że w taki sposób zachowuje się protokół TNS (Net8, SQL*Net) na platformach Windows. Innymi protokołami o dynamicznej charakterystyce są np. protokół FTP i DCOM RPC.

Firewalle klasy proxy

Firewalle klasy proxy to firewalle pozwalające na analizę ruchu na wyższych warstwach. Są one w stanie zrozumieć ruch pojedynczych protokołów (np. HTTP, FTP) i dodatkowo filtrować w zależności od zawartości tego ruchu. Jednakże ich możliwości są ograniczone do kilku protokołów, które są rozumiane przez firewall. Jeśli dany protokół nie posiada odpowiedniego modułu na firewallu, to należy zastosować proxy standardowe, co w praktyce sprowadza funkcjonalność firewalla do warstwy TCP. Ponadto możliwości zablokowania danego ataku są uzależnione od tego czy ruch generowany przez atak znacząco różni się od standardowego ruchu danego protokołu.

IDS

IDS (Intrusion Detection System) to system wykrywania prób ataku. Działa on na zasadzie sondy wpiętej w monitorowany segment sieci. Sonda ta powinna otrzymywać cały ruch sieciowy (jego „kopię”) przeznaczony dla monitorowanego systemu. IDS umie wykrywać w monitorowanym ruchu objawy charakterystyczne dla prób ataku. W wielkim uproszczeniu działa on podobnie do systemu antywirusowego. Porównuje analizowany ruch z bazą sygnatur ataków, która jest integralną częścią IDS. Aktualność tej bazy decyduje o skuteczności IDS. Współczesne produkty IDS pozwalają na zdalne aktualizacje bazy sygnatur ataków. Drugim ważnym aspektem wpływającym na skuteczność IDS jest dostrojenie systemu do charakterystyki monitorowanego ruchu. IDS niezestrojony będzie generował dużą ilość fałszywych alarmów i informacji o niewielkim stopniu ważności. W powodzi informacji może zginać wiadomość o faktycznym ataku.

Po wykryciu potencjalnego ataku, standardowy IDS może zarchiwizować podejrzany ruch sieciowy i zawiadomić administratora.

Jak wynika z powyższego opisu, IDS jest urządzeniem pasywnym. Umie wykryć atak, ale podjęcie akcji należy już do administratora. Jeśli administrator nie będzie w stanie podjąć kroków natychmiastowo, to atakujący może mieć wystarczająco dużo czasu żeby dokonać ataku i zatrzeć po sobie ślady. W związku z powyższym współczesne IDS są coraz częściej wyposażane w możliwości proaktywnej reakcji na atak. Typową opcją jest wyposażanie IDS w moduł integrujący go z zewnętrznym firewalllem. Dokładniej zostanie to opisane w kolejnym rozdziale.

Dlaczego te systemy nie wystarczają?

Firewalle – Działanie na niskim poziomie

Jak już wcześniej wspomniałem firewalle mogą okazać się nieskuteczne w wielu zastosowaniach, ze względu na ograniczenie analizy ruchu do 4 warstwy protokołów (TCP, UDP). W związku z tym nie mogą one wykryć i zablokować ataków wysokopoziomowych.

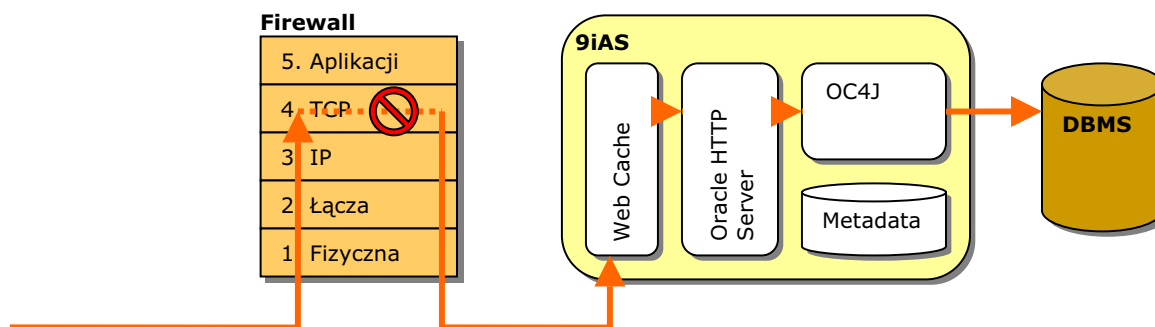
Typowym przykładem jest atak na aplikację internetową. Załóżmy że mamy serwer aplikacyjny Oracle 9iAS udostępniający dane za pomocą aplikacji WWW. Typem klienta, który nas interesuje jest przeglądarka WWW. Podstawową metodą komunikacji z serwerem aplikacji jest przekazywanie stron HTML lub dokumentów XML przez protokół HTTP.

Jeżeli na drodze między przeglądarką a serwerem aplikacji będzie stał firewall, to dla niego ruch aplikacji internetowej będzie zwykłym ruchem HTTP lub HTTPS. Tradycyjne firewalle analizują tylko trzecią i czwartą warstwę protokołów sieciowych. W naszym wypadku są to protokoły IP i TCP. Firewall może filtrować ruch tylko na podstawie:

- źródłowego i docelowego adresu IP
- źródłowego i docelowego numeru portu TCP
- stanu sesji TCP (tylko firewalle statefull inspection)

Jak widać tradycyjne firewalle nie są w stanie reagować na ataki wysokopoziomowe na same aplikacje internetowe. Dla nich ruch HTTP będący atakiem jest nie do rozróżnienia od zwykłego, dozwolonego ruchu HTTP gdyż nie analizują one zawartości sesji HTTP.

Poniższy schemat pokazuje analizę ruchu do aplikacji internetowej przez tradycyjny firewall:



IDS – Niewystarczające możliwości reakcji na naruszenie bezpieczeństwa

Jak już wcześniej wspomniałem, współczesne IDS są coraz częściej wyposażane w możliwości proaktywnej reakcji na atak. Typową opcją jest wyposażanie IDS w moduł integrujący go z zewnętrznym firewallem. W razie wykrycia próby ataku, IDS jest w stanie zdalnie zrekonfigurować firewall tak żeby blokował on ruch z adresu podejrzanego o atak. Rozwiązanie to bywa skuteczne, jednak według mnie nie jest zbyt praktyczne gdyż jednocześnie, zastosowanie takiej integracji firewalla i IDS otwiera nowe możliwości ataków. Np. atakujący może podszyć się pod adres IP centrali firmy czy też popularnego portalu

i z takiego adresu IP zasymulować atak. Spowoduje to zablokowanie dostępu do tego zasobu. Poza tym rozwiązanie to nie zawsze jest skuteczne. Współczesne metody ataku opierają się na działaniu wielostopniowym, zawierającym akcje rozpoznawcze, przygotowanie ataku i sam atak. Często stosowaną metodą jest prowadzenie rozpoznania i przygotowania z innych adresów źródłowych niż sam późniejszy atak, lub ukrywanie zasadniczego ataku w powodzi pakietów symulujących zmasowany atak innego rodzaju, z wielu różnych źródeł.

Firewalle aplikacyjne

Tradycyjne firewalle sieciowe nie są w stanie sprostać ochronie aplikacji internetowych. W związku z tym, ostatnio pojawiła się nowa klasa oprogramowania – firewalle aplikacyjne.

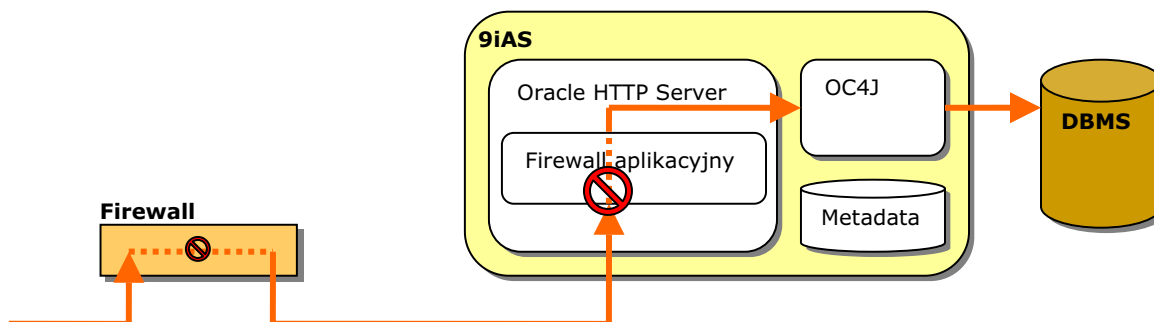
Firewall aplikacyjny to rodzaj filtru integrującego się z serwerem WWW. Działa on między częścią sieciową serwera, a częścią aplikacyjną. W związku z tym dostaje do analizy ruch po wstępnej obróbce przez serwer, tak jak go będą widziały dalsze warstwy. Serwer WWW zajmuje się:

- rozszyfrowaniem transmisji SSL (jeśli jest używana),
- zdekodowaniem zlecenia (jeśli było stosowane np. kodowanie hexadecymalne URI),
- wstępną obróbką zlecenia.

Firewalle aplikacyjne działając jako moduł serwera WWW bardzo blisko się integrują z serwerem aplikacji. Dzięki takiemu rozwiązaniu:

- nie muszą dbać o szyfrowanie SSL
- nie da się ich obejść, przez zakodowanie zlecenia
- mogą być to stosunkowo proste mechanizmy, gdyż sporą część pracy wykonuje za nie serwer WWW.

Poniższy schemat przedstawia umiejscowienie firewalla aplikacyjnego w architekturze serwera aplikacji.



Praktycznie każdy współczesny serwer WWW posiada możliwość rozszerzania swojej funkcjonalności przez dodawanie modułów:

- dla serwera Microsoft ISS są to filtry ISAPI
- dla Apache są to moduły Apache
- dla Netscape/iPlanet/SunOne są to moduły iAPI

Oracle HTTP Server będący elementem Oracle 9iAS to standardowy serwer Apache 1.3.x. Posiada on możliwość ładowania modułów dynamicznych, tworzonych w postaci

bibliotek. Tak więc powinien dobrze integrować się z rozwiązaniami stworzonymi dla Apache.

Niestety jak narazie nie znam firewalla aplikacyjnego dedykowanego dla Oracle Application Server. Rozwiązania przygotowane dla Apache 1.3 powinny działać, jednakże nie są to konfiguracje w jaki kolwiek sposób wspierane przez Oracle.

Intrusion Protection System / IDS-inline

Obecnie zauważa się tendencje do rozbudowywania firewallei o funkcje wykrywania prób ataków i tendencje do stosowania IDS-ów w zastosowaniach tradycyjnie przeznaczonych dla firewallei. Obie te technologie zaczynają przenikać się. Świetnie to widać w ruchach liderów technologii IDS i firewall.

Obecnie coraz częściej mówi się o IPS – Intrusion Protection Systems. Są to systemy IDS rozbudowane o możliwości aktywnej reakcji na wykryte zdarzenia. Pierwszym ruchem zmierzającym do rozszerzenia możliwości reakcji standardowego systemu IDS było pojawienie się technologii przerywania połączeń. W skrócie, współczesne IDS-y mogą w przypadku wykrycia podejrzanego połączenia TCP przerwać to połączenie przez podszycie się pod stronę atakującą i wysłanie pakietu TCP z flagą RST. Pakiet z taką flagą oznacza zakończenie połączenia. Tak więc atakowany serwer zakończy połączenie i atak nie będzie mógł dojść do skutku. Technika ta jest skuteczna przy atakach angażujących całą sesję TCP. Nie zadziała np. dla ataków składających się z jednego pakietu i ataków przenoszonych przez inne protokoły niż TCP, w szczególności – protokoły bezstanowe.

Kolejnym – rewolucyjnym krokiem, jest IDS-inline. O ile tradycyjny IDS ma jedną kartę sieciową, która jest sondą wpinaną w monitorowaną sieć, to IDS-inline posiada dwie karty – zewnętrzną i wewnętrzną. Cały monitorowany ruch sieciowy przechodzi przez urządzenie. Przypomina to budowę firewallei, jednak w środku działa silnik IDS, który wykrywa ataki i umie je blokować. W sumie urządzenie pełni podobne funkcje jak firewall jednakże działa w inny sposób. Firewalle to technologia restryktywna. Blokują one cały ruch z wyjątkiem ruchu dozwolonego. Istotą działania IDS jest wykrywanie prób ataku, w związku z tym IDS-inline chociaż jest umieszczony w tym samym miejscu co firewall, to działa w ten sposób, że przepuszcza cały ruch z wyjątkiem tego co uzna za próbę ataku.

W przypadku IDS-inline klasyfikacja aktywności sieciowej jest o wiele bardziej zaawansowana niż w przypadku firewallei. IDS stosuje do tego wiele technologii. Ogólnie mówi się że IDS-y działają na podstawie dopasowywania sygnatur ataków. Jest to duże uproszczenie. W żadnym wypadku nie oznacza to że IDS ma dokładny wzorzec każdego ataku i z taką bazą danych konfrontuje nadzorowany ruch. Jeśli by tak było, to IDS-y dałoby się bardzo łatwo oszukać. Przykładowo jeśli IDS analizowałby zapytania SQL, to wstawienie jednej lub więcej spacji spowodowałoby brak dopasowania reguły i udałoby się obejść zabezpieczenie. W rzeczywistości współczesne IDS-y stosują wiele różnych technik detekcji prób ataku. Np. normalizatory i interpretery poszczególnych protokołów, sygnatury opisowe w miejsce konkretnych wzorców, oraz metody heurystyczne.

Mimo to technologia IDS-inline (IPS) nie jest w stanie zastąpić w pełni firewallei. Chociażby dlatego że nie może to być technologia działająca na zasadzie restryktywności. Dlatego też rynek IPS będzie prawdopodobnie rozwijał się w kierunku rozwiązań hybrydowych, w których funkcjonalność IDS-inline będzie uzupełniana przez tradycyjny firewall statefull inspection. Specjalizacja w urządzeniach ochronnych będzie uzależniona od miejsca w których one działają a nie od techniki jaką stosują. Przykładowo, na froncie będzie działał IPS wykorzystujący IDS-inline i zintegrowany firewall, a wewnątrz sieci

IPS zintegrowany w przełączniku sieciowym (mówi się już o takich projektach) bazujący na technologii wieloportowego IDS-inline.

Podsumowanie

W najbliższym czasie można spodziewać się prawdziwych rewolucji na rynku zabezpieczeń przed atakami z sieci. Powinno to pozwolić na zmniejszenie luki spowodowanej dynamicznym rozwojem technologii, za którą współczesne zabezpieczenia często nie nadążają. Mam nadzieję że mój wykład przybliżył Państwu obecne i przyszłe technologie i pozwoli na dokonywanie rozsądniejszych inwestycji. Pamiętajmy że najpierw należy dobrze poznać technologię, jej zalety i ograniczenia, a później przystąpić do wyboru rozwiązania. Ważne jest również (nawet ważniejsze od samego wyboru produktu) właściwe jego skonfigurowanie. Testowane przez nas instalacje produktów zabezpieczających często sprawiają wrażenie, że spodziewano się że nabyto „cudowne pudełko” które samo z siebie załatwi wszystkie problemy. Pamiętajmy – to są tylko narzędzia, trzeba jeszcze ich użyć w sposób świadomy. Tak czy inaczej – intruzi łakomi na nasze dane będą mieli wkrótce ciężki orzech do zgryzienia.