

Bezpieczny Serwer WWW

Daniel Letkiewicz
Politechnika Wrocławska, Instytut Cybernetyki Technicznej
e-mail: dletkiew@ict.pwr.wroc.pl

Abstrakt: Rosnąca liczba włamań do serwerów WWW skłania do poszukiwania nowych metod zabezpieczania usługi WWW. Jednym z rozwiązań może być zastosowanie specjalizowanych urządzeń, które będąc prostym serwerem WWW, obsługują dane szczególnie podatne na ataki włamywaczy komputerowych. Ich bezpieczeństwo nie opiera się na stosowaniu kolejnych zabezpieczeń ale na wyeliminowaniu mechanizmów, które mogą zostać wykorzystane przez włamywaczy.

1. Wstęp

World Wide Web jest już od dawna jedną z najbardziej popularnych usług dostępnych w sieci Internet. Za jej pośrednictwem publikowane są ogromne ilości informacji, które może przeczytać każdy kto ma dostęp do „globalnej sieci”. WWW wykorzystują zarówno osoby prywatne, publikując np. zdjęcia z ostatnich wakacji, jak również bardzo poważne instytucje, które używają WWW do rozpowszechniania cennych informacji.

Jednym z problemów, z którym borykają się administratorzy serwerów WWW jest zapewnienie bezpieczeństwa udostępnianych danych, a przede wszystkim odpowiednie zabezpieczenie ich przed nieuprawnionym zmodyfikowaniem.

Bardzo często główna strona serwisu WWW jest swego rodzaju wizytówką, która ma m.in. przedstawić serwis i zachęcić do dalszej eksploracji. Jak wykazują statystyki, w wyniku włamania do serwera, najczęściej zmieniana jest właśnie główna strona serwisu, gdyż jest ona najczęściej oglądana, a to przynosi popularność i satysfakcję włamywaczowi.

Motywy, jak również skutki włamań komputerowych do serwerów WWW mogą być bardzo różne i trudno jest je tutaj w skrócie sklasyfikować lub nawet wymienić. Jednakże, najczęściej skutkiem włamania będzie umieszczenie mniej lub bardziej dowcipnych tekstów przez „poszukiwaczy wrażeń”, którzy kolekcjonują kolejne „zhackowane site-y”. Skutkiem takiego włamania jest utrata reputacji i kompromitacja serwisu WWW. Mogą zdarzyć się również włamania wykonywane na zamówienie przez zawodowych włamywaczy, o których właściciele serwisu mogą się nigdy nie dowiedzieć. W takich przypadkach najczęściej celem wtargnięcia jest kradzież danych, które przeznaczone są dla wąskiego grona odbiorców.

2. Bezpieczeństwo usługi WWW

Serwer WWW uruchomiony jest na jednostce, która stanowi element większego systemu komputerowego komunikującego się za pośrednictwem sieci. Rozważając bezpieczeństwo usługi WWW należy wziąć pod uwagę wszystkie aspekty bezpieczeństwa dotyczące całej infrastruktury systemu komputerowego, w której znajduje się serwer.

2.1. Klasyfikacja bezpieczeństwa

Bezpieczeństwo usługi WWW można podzielić na następujące obszary:

- **bezpieczeństwo fizyczne** - czasami łatwiej jest po prostu ukraść komputer lub dysk niż zdalnie uzyskać nieautoryzowany dostęp do chronionych zasobów. Nieuczciwej firmie może bardziej opłacać się przekupić niełojalnego pracownika niż wynajmować włamywacza komputerowego.

- **bezpieczeństwo infrastruktury sieciowej** - pomiędzy serwerem WWW a przeglądarką bardzo często jest spora odległość (nie tylko w sensie fizycznym). Serwer WWW może być niezdożyta fortecą ale na niewiele się to przyda, gdy atakujący przechwyci lub przekieruje połączenie pomiędzy przeglądarką a serwerem. Podszrywając się pod prawdziwy serwis może próbować wydobyć cenne informacje lub okłamać osobę, która nie zdaje sobie sprawy, że „rozmawia” z oszustem. Włamywacz może również wykorzystać słabo zabezpieczone lub niewłaściwie skonfigurowane komputery, mające uprzywilejowany dostęp do maszyny serwera WWW.
- **bezpieczeństwo systemu operacyjnego i usług sieciowych** ma ogromny wpływ na bezpieczeństwo serwera WWW. Bezpieczeństwo systemu komputerowego można porównać do łańcucha, który jest tak wytrzymały jak najsłabsze z jego ogniw. Włamywacz może wykorzystać słabości systemu operacyjnego, przestarzałe i zawierające błędy lub po prostu źle skonfigurowane usługi dostępne poprzez sieć. Niezapewnienie należytego bezpieczeństwa w tym obszarze jest najczęstszą przyczyną włamań.

2.2. Zapewnianie bezpieczeństwa

Do dnia dzisiejszego powstało wiele rozwiązań, które mogą zostać zastosowane w celu zapewnienia jak najwyższego poziomu bezpieczeństwa poszczególnych, ww. obszarów. Rozwiązania te są ciągle rozwijane i udoskonalane.

Nad bezpieczeństwem fizycznym czuwają specjalne organizacje i systemy ochrony.

Istnieje wiele dokumentów i zaleceń dotyczących zabezpieczeń infrastruktury sieciowej, począwszy od etapu projektowania sieci, aż do konfiguracji poszczególnych urządzeń i usług sieciowych.

Największym zagrożeniem dla systemów operacyjnych i usług sieciowych są nowo odkrywane błędy programistyczne mające wpływ na bezpieczeństwo systemu. Dlatego też, zaleca się aby ciągle uaktualniać oprogramowanie i stosować poprawki eliminujące ujawnione błędy. Dostępnych jest wiele rozwiązań, wykorzystujących m.in. kryptografię, mających na celu podniesienie poziomu bezpieczeństwa zarówno systemu operacyjnego jak i poszczególnych usług sieciowych. Wdrażanie nowych, wyrafinowanych metod ochrony, odkrywanie błędów i stosowanie kolejnych poprawek wydają się być drogą do doskonałości, która nigdy nie będzie miała końca.

3. Bezpieczny serwer WWW

Zostawiając bezpieczeństwo fizyczne wyspecjalizowanym systemom ochrony, bezpieczeństwo infrastruktury sieciowej projektantom i administratorom sieci, przyjrzyjmy się bliżej bezpieczeństwu urządzenia, na którym pracuje serwer WWW.

Duży, skomplikowany serwer, obsługujący CGI, realizujący usługę poczty elektronicznej, FTP, operujący na rozproszonych bazach, używający technologii ASP czy PHP itp. jest trudny w konfiguracji i może zawierać błędy mające wpływ na jego bezpieczeństwo.

Główne strony serwisu, które są celem ataków włamywaczy, zawierają raczej informacje statyczne, tzn. że raz zaprojektowane nie zmieniają się zbyt często i jako takie nie muszą być obsługiwane przez skomplikowane serwery. Udostępnianiem tych informacji może zająć się zatem specjalizowane urządzenie, którego głównym celem jest ochrona integralności przechowywanych danych. Bezpieczeństwo takiego urządzenia opiera się na jak największym uproszczeniu zarówno systemu operacyjnego jak i programu serwera WWW, zgodnie z zasadą, że:

NIE MOŻNA DOKONAĆ CZEGOŚ CO JEST FIZYCZNIE NIEMOŻLIWE.

Zamiast zabezpieczać informacje przed zmodyfikowaniem lepiej jest zupełnie usunąć możliwość modyfikacji danych z systemu, pozostawiając tylko to co jest niezbędne do pracy programu serwera WWW.

3.1. Cechy bezpiecznego serwera WWW

Urządzenie pracuje pod kontrolą systemu operacyjnego Linux, ponieważ jest to wysoce skalowalny i bardzo elastyczny system. Wyposażone jest w pamięć flash zawierającą system operacyjny oraz w czytnik płyt CD, na których przechowywane są dane udostępniane przez WWW.

Bezpieczny serwer posiada dwa tryby pracy, które wybierane są przy starcie urządzenia:

- **konfiguracyjny**, w którym możliwe jest tylko i wyłącznie ustawienie parametrów konfiguracyjnych i zapisanie ich w specjalnie przygotowanym miejscu na pamięci flash.
- **serwerowy**, w którym urządzenie pracuje jako serwer WWW.

Każdy z tych trybów posiada własne, odpowiednio przystosowane, jądro systemu oraz własny system plików, który zawiera tylko to co jest niezbędne do pracy danego trybu.

Szczególny nacisk został położony na bezpieczeństwo systemów plików. Znajdują się one, wraz z kernelami, na osobnej partycji w postaci skompresowanej, w pamięci flash. Po starcie ładowane są bezpośrednio do pamięci operacyjnej i rezydują tam aż do zresetowania urządzenia. Skompresowane dane na flashu nigdy nie są modyfikowane, po za tym w systemie plików nie ma, żadnych dodatkowych programów ani bibliotek, które mogłyby posłużyć do takiej modyfikacji.

Zapis do pamięci flash możliwy jest tylko w trybie konfiguracyjnym i tylko na wydzielonej partycji. Tryb serwerowy został pozbawiony tej możliwości poprzez usunięcie niskopoziomowych procedur obsługujących pamięci flash z jądra systemu. Tryb konfiguracyjny natomiast został pozbawiony mechanizmów obsługujących sieć komputerową, dzięki czemu zdalna modyfikacja pamięci flash jest niewykonalna.

Dane udostępniane przez serwer WWW są zabezpieczone przed modyfikacją poprzez umieszczenie ich na płycie CD, na której zapis jest fizycznie niemożliwy.

Program serwera WWW został uproszczony do tego stopnia, że nie jest wymagana jakakolwiek jego konfiguracja. Pozbawiony nawet takich mechanizmów jak CGI czy serwery wirtualne nie daje zbyt dużych możliwości włamywaczom. Jest on jednocześnie na tyle funkcjonalnym, aby sprawnie obsługiwać dane umieszczone na płycie CD. Proces serwera pracuje w systemie z minimalnymi uprawnieniami pozwalającymi jedynie na odczytu danych udostępnianych przez WWW.

Konfiguracja ogranicza się jedynie do podania parametrów niezbędnych do komunikacji za pomocą protokołu IP. Wymiana danych udostępnianych przez WWW sprowadza się do wymiany płyty CD, w dowolnym momencie pracy serwera. Gdy w napędzie nie ma CD, serwer WWW zwraca do przeglądarki odpowiednią informację o chwilowej niedostępności danych. Raz skonfigurowane urządzenie nie wymaga praktycznie żadnej ingerencji ze strony administratora.

3.2. Przeznaczenie

Serwer przeznaczony jest do obsługi danych, które nie wymagają zbyt częstych modyfikacji, gdyż każdorazowa zmiana wiąże się z koniecznością nagrywania nowej płyty CD. Główne strony serwisów doskonale nadają się do umieszczenia na tego typu urządzeniu. Jeżeli istnieje konieczność używania zaawansowanych technologii, takich jak ASP, PHP czy servlety Javy zawsze można zaprojektować serwis tak, aby główne strony były statyczne a pozostałe dane można umieszczać na dowolnym, ulubionym serwerze WWW. W ten sposób główny cel włamywaczy będzie zabezpieczony, a cały serwis będzie posiadał dowolną funkcjonalność.

3.3. Zagrożenia bezpieczeństwa

Mimo, że bezpieczny serwer WWW w znaczny sposób podnosi bezpieczeństwo przechowywanych informacji, to nie jest on rozwiązaniem gwarantującym stuprocentowe bezpieczeństwo. Istnieje pewne prawdopodobieństwo, zmodyfikowania danych udostępnianych przez WWW, np. poprzez manipulacje pamięcią cache lub modyfikację programu serwera WWW,

znajdującego się w pamięci RAM. Jednakże brak mechanizmów i programów w systemie, które mogłyby zostać do tego celu wykorzystane, sprawia że prawdopodobieństwo to jest bliskie zera.

4. Podsumowanie

Rozwój technik i metod stosowanych w World Wide Web sprawia, że serwery WWW stają się coraz bardziej skomplikowane, a tym samym podatne na błędy i trudne w konfiguracji. Alternatywą dla skomplikowanych zabezpieczeń mogą stać się dedykowane systemy, które przejmą część zadań i zasobów szczególnie wrażliwych na ataki włamywaczy komputerowych. Przeznaczone do realizacji pojedynczej, konkretnej usługi mogą zostać pozbawione niepotrzebnych mechanizmów w znacznym stopniu ograniczając pole działania włamywaczom komputerowym.

Stosowanie dedykowanych urządzeń nie jest nowym pomysłem, a wdrożenie ich nie zawsze jest rzeczą łatwą. Jednakże wzrost przestępczości komputerowej pozwala przypuszczać, że w przyszłości na nich będzie opierać się większość usług dostępnych w sieci Internet.