

Konferencja:

V Kongres Bezpieczeństwa Sieci. Warszawa, 24.02.2009r.

Blok: Firewall & VPN GigaCon.

Temat prezentacji:

Firewall aplikacyjny jako jeden z elementów zabezpieczenia aplikacji WWW.

Streszczenie prezentacji:

W trakcie prelekcji prowadzonej przez Michała Sajdaka słuchacze zapoznają się z ideą firewalla aplikacyjnego. Pojęcie to zostanie zaprezentowane w kontekście zyskujących coraz większą popularność aplikacji webowych (WWW). W trakcie prezentacji zostaną wskazane zagrożenia dla tego typu oprogramowania oraz metody ochrony oferowane przez dedykowane firewalły aplikacyjne.

Ponadto, w trakcie sesji, uczestnicy będą mogli uzyskać odpowiedzi na pytania: jakie różnice istnieją pomiędzy firewallem aplikacyjnym a klasycznym firewallem sieciowym? O czym warto pamiętać wdrażając firewall aplikacyjny? Jakie inne, komplementarne techniki można stosować aby zabezpieczyć system IT przed atakami?

O prelegencie:

Michał Sajdak - Dyrektor ds. Rozwoju w firmie Securitum, specjalizującej się w wykonywaniu testów bezpieczeństwa aplikacji i infrastruktury oraz konsultingu w zakresie bezpieczeństwa danych. Wcześniej pracował jako Dyrektor IT w firmie WebService (grupa SOLIDEX). Posiada wieloletnie doświadczenie w obszarach: IT security oraz Software. Wykonywał audyty bezpieczeństwa – w tym testy penetracyjne – dla największych organizacji w Polsce. Interesuje się tematyką bezpieczeństwa aplikacji - ze szczególnym naciskiem na aplikacje WWW.

Aplikacje WWW – krótka charakterystyka

- Wprowadzenie
 - Przykłady. Bankowość elektroniczna, portal internetowy, intranet, ekstranet.
 - Architektura. Klient-serwer, standaryzacja.
 - Umieszczenie protokołu http w modelu OSI. Powyżej warstwy sieci i transportu - warstwa aplikacji.
- Zagrożenia dla aplikacji WWW
 - Ataki hackerskie.
 - Ataki zautomatyzowane – robaki (ang. *worms*).
 - Ataki wykonywane przez pracowników.
 - Inne.
- Najczęstsze typy błędów
 - Ataki na serwer. SQL Injection, malicious file execution, ...
 - Ataki na klienta. XSS (Cross Site Scripting), XSRF (Cross Site Request Forgery), ...
 - Błędy logiczne.

Ochrona aplikacji WWW - firewalły

- Klasyczne firewalły sieciowe
 - Chronią przed zagrożeniami w warstwie sieciowej.
 - Najczęściej nie filtrują dokładnie ruchu http/https.
 - Nie chronią przed atakami odbywającymi się w warstwie aplikacji.
- Firewalły aplikacyjne
 - Specjalizowane do ochrony określonego typu protokołu w warstwie aplikacji (np. http).
 - Wykonują wnikliwą analizę komunikacji – dla chronionego protokołu.
 - Nie zabezpieczają przed zagrożeniami w warstwie sieciowej.
- Tryby działania
 - Pasywny (wykrywanie zagrożeń i ich logowanie).
 - Aktywny (wykrywanie i aktywne blokowanie zagrożeń).
 - Tryb nauki (pasywne tworzenie reguł na podstawie analizowanego ruchu sieciowego).

Charakterystyka firewala aplikacyjnego

- Rodzaj zapewnianej ochrony
 - Sygnatury. Blacklisting. Whitelisting.
 - Dodatkowa warstwa zabezpieczeń aplikacyjnych.
 - Accounting.
 - OWASP Top 10 ? PCI DSS ?
- Sposoby konfiguracji
 - Prekonfigurowane ustawienia.
 - Tryb nauki.
 - Konfiguracja ręczna.
 - Wydajność. Terminacja sesji SSL, clustering, load balancing.
- Zalety firewala aplikacyjnych
 - Możliwość szybkiej ochrony aplikacji, bez konieczności jej zmiany.
 - Relatywnie szybki i elastyczny kosztowo sposób zapewnienia ochrony dla aplikacji.
 - W zasadzie jedyny sposób ochrony aplikacji, dla której nie ma dostępnych kodów źródłowych/nie ma wsparcia producenta.
 - Relatywnie łatwa startowa konfiguracja.
 - Istotny element składający się na całościową ochronę systemu IT.
 - Dostępne w wersji hardware oraz software.
- Wady firewala aplikacyjnych
 - Pełna konfiguracja – trudna i wymagająca specjalistycznej wiedzy.
 - Duży wpływ na wydajność. Dodatkowy potencjalny punkt awarii.
 - Fałszywe alarmy. Powodujące konieczność rozluźnienia konfiguracji i zmniejszenia ochrony.
 - Przy niepoprawnej konfiguracji – negatywny wpływ na funkcjonalności biznesowe chronionej aplikacji.
 - Brak ochrony dla wielu typów błędów.
 - Wysoka cena. Zakup licencji, koszty pracownicze, wsparcie, utrzymanie.

Przykłady firewala aplikacyjnych

- Sprzętowe
 - F5 BIG-IP ASM
 - Cisco ACE Web Application Firewall
 - Armorlogic Profense
- Programowe
 - Armorlogic Profense
 - mod_security
 - WebKnight

Komplementarne środki ochrony

- Poprawny kod aplikacji i narzucenie bezpiecznej architektury systemu.
- Testy/audyty bezpieczeństwa.
- Hardening infrastruktury. Hardening sieci.
- Edukacja pracowników.
- Stały monitoring całości systemu.
- Zabezpieczenia proceduralne (polityka bezpieczeństwa, standardy, procedury).

Podsumowanie

- Firewalle aplikacyjne działają w innej warstwie komunikacji niż znane, klasyczne firewalle sieciowe.
- Firewalle aplikacyjne są wyjątkowo użyteczne jeśli przedsiębiorstwo nie posiada dostępu do kodów źródłowych/nie posiada wsparcia producenta dla aplikacji wymagającej ochrony.
- Podstawowa konfiguracja jest relatywnie prosta.
- Precyzyjna konfiguracja jest skomplikowana i wymagająca specjalistycznej wiedzy z zakresu bezpieczeństwa aplikacji.
- Firewalle aplikacyjne w połączeniu z dodatkowymi środkami zabezpieczeń, zapewniają optymalną ochronę systemu IT.