

Bezpieczeństwo webowej aplikacji

Firma Phion przedstawiła nowe urządzenie ochrony aplikacji WWW z inspekcją w warstwach 7 i 8 – Airlock.

Dzisiejsze aplikacje powszechnie wykorzystują interfejs webowy. Chociaż jest to bardzo wygodne, trudno zapewnić takim aplikacjom wymagany poziom bezpieczeństwa. Wynika to stąd, że dla klasycznej zapory, cały ruch odbywa się w standardowych sesjach HTTP, na porcie 80 lub wewnątrz szyfrowanego połączenia SSL. Aby móc chronić aplikację i serwer przed atakami, rozwiązanie ochronne powinno rozpoznawać nie tylko protokół, ale także dane przesyłane od aplikacji do klienta i z powrotem.

Przyjrzyć się zapytaniom, nie pakietom

Airlock jest produktem szwajcarskiej firmy Visonys, obecnie połączonej z austriacką firmą Phion. Rozwiązanie to jest dostępne jako paczka oprogramowania lub gotowe urządzenie typu appliance, wykorzystuje system operacyjny Solaris, włącznie z jego mechanizmami zabezpieczeń (zony). Zadaniem Airlocka jest

Zadaniem Airlocka jest kontrola dostępu i ochrona serwera internetowego przed atakami z zewnątrz przez analizę protokołu WWW. Analizie wewnątrz protokołu podlegają aplikacje Web 2.0, formularze przesyłane do serwera i z powrotem oraz kod AJAX.

kontrola dostępu i ochrona serwera internetowego przed atakami z zewnątrz przez analizę protokołu WWW. Analizie wewnątrz protokołu podlegają aplikacje Web 2.0, formularze przesyłane do serwera i z powrotem oraz kod AJAX. Urządzenie może także służyć do terminowania ruchu SSL, odciążając serwer webowy, wspiera różne metody uwierzytelnienia (LDAP, Radius, RSA, OCSP, Kerberos i certyfikat w przeglądarce) oraz umożliwia konfigurację o wysokiej dostępności. Urządzenie jest licencjonowane na chronione aplikacje.

Za pomocą rozwiązania, które umie analizować dane wymieniane podczas pracy z aplikacją, można odfiltrować najważniej-

MARCIN MARCINIAK

sze ataki takie, jak SQL Injection, Cross Site Scripting, wykonanie podstawionego pliku, podmiana danych formularza, niezabezpieczone odwołania do obiektów pobierania danych, modyfikacja linków, błędy autoryzacji i szyfrowania danych, wyciek oraz nieprawidłowa obsługa błędów. Zadaniem takiego zabezpieczenia nie jest wykrycie błędów, ale blokowanie odwołań, które nie pasują do modelu eksploatacji aplikacji.

Uwaga na formularze

Przy normalnej pracy aplikacji webowej, zwracane wartości pól wyboru mogą przyjmować tylko wskazane w formularzu wartości. Każda ich modyfikacja oznacza atak i jest blokowana. To samo dotyczy linków. Przy wyborze dozwolonych akcji stosuje się dwie listy – białą i czarną. Biała zawiera cechy, z których przynajmniej jedna musi być spełniona przez zapytanie przekazywane do serwera. Przykładem reguły może być ograniczenie: „dla danego formularza obsługujemy wyłącznie POST z konkretnej grupy adresów IP”. Czarna lista zawiera wszystko, co jest zakazane – sygnatury XSS, SQL Injection, Code Injection, przepelnień bufora i własne filtry użytkowników.

Odfiltrowanie ataków polega nie tylko na wykryciu i zablokowaniu znaków, które wskazują na próbę wstrzyknięcia kodu, ale także na tym, że system zabezpieczeń odróżnia niestandardową odpowiedź, która nie może pochodzić od przeglądarki. Zabezpieczane są pola ukryte (HIDDEN), sprawdzana jest długość pól oraz zgodność ze wzorcem wartości. W ten sposób działają także urządzenia firmy F5.

Zabezpieczyć linki

Nawigacja pomiędzy podstronami serwisu odbywa się za pomocą linków. Niektóre aplikacje mogą posiadać ukryte obiekty, do których nie prowadzi żaden link, ale strony lub obiekty istnieją i mogą zostać wywołane. Przykładem może być link, w którym odwołanie odbywa się za pomocą przekazania parametru. Atak polegający na zmianie wartości takiego parametru jest trudny do wychwycenia w strumieniu informacji z logów serwera, ale urządzenie analizujące pracę aplikacji potrafi go wykryć.

Najbezpieczniejszym sposobem blokowania takich ataków jest szyfrowanie odwołań.

Przed jakimi atakami chroni Airlock?

- SQL Injection
- Cross Site Scripting
- Wykonanie podstawionego pliku
- Podmiana danych formularza
- Niezabezpieczone odwołania do obiektów pobierania danych
- Modyfikacja linków
- Błędy autoryzacji i szyfrowania danych
- Wyciek oraz nieprawidłowa obsługa błędów

Jawne linki serwera są przekształcane kryptograficznie tak, by każda modyfikacja była łatwa do wykrycia. Urządzenie potrafi linki podmieniać podczas przeglądania, w locie, dzięki czemu każda modyfikacja obiektu będzie wykryta i zablokowana. Akcją blokady może być przeniesienie na stronę główną serwisu, wygaszenie sesji i zablokowanie wszelkiego już dokonanego uwierzytelnienia.

Airlock – dzięki temu, że analizuje ruch przechodzący – potrafi wykryć także ataki pośredniczące CSRF (*Cross Site Request Forgery*). Polegają one na użyciu przeglądarki użytkownika do ataku na inną aplikację, do której atakujący nie ma dostępu. W ten sposób

W zastosowaniach wymagających szczególnie wysokiego poziomu bezpieczeństwa warto wdrożyć technologie client fingerprinting.

można pobrać informację z firmowej aplikacji w Intranecie z zewnątrz przy użyciu odpowiednio spreparowanego skryptu. Tego typu ataki spotyka się dość rzadko, ale w przypadku środowisk o wysokich wymaganiach odnośnie do bezpieczeństwa, należy je uwzględnić.

Kto naprawdę się łączy?

W zastosowaniach wymagających szczególnie wysokiego poziomu bezpieczeństwa warto wdrożyć technologię kontroli stacji roboczej, z której łączy się dany użytkownik. Metoda zwana *client fingerprinting* zabezpiecza przed przejściem sesji, sprawdzając informacje wysyłane przez przeglądarkę do serwera, takie jak identyfikacja przeglądarki, informacja o systemie operacyjnym, rozdzielczości ekranu itd. Dla każdego z pól można przypisać odpowiednią wagę, po przekroczeniu zadanych wartości następuje akcja – logowanie, powiadomienie aplikacji, przerwanie połączenia i zablokowanie sesji. Kontrola klienta wykryje większość typowych ataków, gdzie przestępcy nie udaje się symulować wszystkich parametrów komputera ofiary. Jeśli atakujący nie zastosuje tej samej przeglądarki co ofiara, prawdopodobieństwo wykrycia ataku jest bardzo wysokie. ▀