Wymagania ogólne
Dostawa systemu ochrony aplikacji webowych oraz API, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe, a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń.

1. System powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej lub programowej.
2. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia.
3. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Architektura systemu

1. Dla zapewnienia wysokiej sprawności i skuteczności działania, wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa.
2. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe, zastosowane w nich technologie oraz platforma sprzętowa pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie.
3. Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent.
4. Produkt nie może posiadać ograniczeń co do liczby chronionych aplikacji web.
5. Powinna istnieć możliwość zdefiniowania co najmniej 16 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami systemu.
6. System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active.

Parametry fizyczne systemu

1. System realizujący funkcje podstawowe musi dysponować minimum:
   - 4 portami Gigabit Ethernet RJ-45.
   - 4 gniazdami SFP 1 Gbps.
   - 4 gniazdami SFP+ 10 Gbps.
2. Powierzchnia dyskowa - minimum 480 GB typu SSD.
3. Obudowa urządzenia o wysokości maksymalnie 2U z możliwością montażu w standardowej szafie teletechnicznej 19 cali.
4. Urządzenie musi być wyposażone w minimum dwa redundantne zasilacze. Musi istnieć możliwość wymiany zasilacza w trakcie pracy urządzenia.
5. Urządzenie musi być fabrycznie nowe.

Parametry wydajnościowe

1. Przepustowość dla ruchu http w warstwie L7 - min 5 Gbps.

Podstawowe funkcje systemu
System musi realizować co najmniej poniższe funkcje:

1. Obsługa protokołów: HTTP 1.1, HTTP 2.0, FTP.
2. Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia:
   - Round Robin,
   - Weighted Round Robin,
   - Least Connection,
   - Source IP Hash,

- URI Hash
- Full URI Hash
- Host Hash
- Host DomainHash

3. Wsparcie dla mechanizmów session persistence:
   - Source IP
   - HTTP Header
   - URL parameter
   - Cookie
   - SSL Session ID

4. Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3.

5. Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa.

6. Ochrona aplikacji www przed takimi zagrożeniami jak:
   - SQL and OS Command Injection.
   - Cross Site Scripting (XSS).
   - Cross Site Request Forgery.
   - Outbound Data Leakage.
   - HTTP Request Smuggling.
   - Buffer Overflow.
   - Encoding Attacks.
   - Cookie Tampering / Poisoning.
   - Session Hijacking.
   - Broken Access Control.
   - Forceful Browsing /Directory Traversal.
   - Ochrona przed innymi zagrożeniami specyfikowanymi przez listę OWASP.
   - Ochrona przed atakami typu Brute force.
   - Ochrona przed atakami clickjacking.
   - Ochrona przed atakami DoS

7. Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację.
8. Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania.
9. Integracja z zewnętrznymi systemami uwierzytelniania dwu-składnikowego.
10. Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy.
11. Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only”.
12. Content routing na bazie parametrów http oraz certyfikatów X.509.
13. Ochrona przed Web Scraping.
14. Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3.
15. Ochrona przed atakami typu SLOW (Slowloris i podobne).
16. Możliwość selektywnego wyłączania blokowania ataków dla sygnatur oraz obszarów aplikacji. Dodanie wyjątków dla sygnatur na podstawie wielu parametrów:
    - Metoda HTTP.
    - IP klienta.
    - Host.
    - URI.
    - Cały URL.

- Parametr.
- Cookie.
- HTTP Header
- JSON Elements

17. Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”.
18. Wszelkie klucze prywatne zapisywane na dyskach urządzenia muszą być zapisywane w postaci zaszyfrowanej.
19. Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.
20. Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML.
21. Wsparcie dla walidacji OpenAPI, JSON i XML.
22. Blokowania „Illegal XML Format” oraz „Illegal JSON Format”.
23. Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy.
24. Przydzielanie różnych certyfikatów dla różnych nazw domenowych.
25. Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate.
26. System musi posiadać możliwość automatycznego uczenia się działania aplikacji w zakresie:
    - obserwacji i budowania profilu dla URL, parametrów, metod HTTP, sesji HTTPS. Obserwacje powinny uczyć model matematyczny normalnych zachowań, który następnie umożliwi wykrywanie anomalii
    - Wyuczony model matematyczny wykrywa odstępstwa od normy w obserwowanych elementach
    - System automatycznie wykrywa zmiany po stronie aplikacji lub zachowania użytkowników i ponawia proces uczenia.
    - Możliwe jest zdefiniowanie wyjątków, które nie będą brały udziału w uczeniu modelu matematycznego
    - Musi istnieć możliwość strojenia czułości modelu wykrywającego anomalie przez administratora systemu. Poziom czułości musi być ustawiany globalnie dla aplikacji jak i na poziomie pojedynczych parametrów.
27. System musi posiadać funkcje ochrony komunikacji API wspieraną technologią uczenia maszynowego. Zakres wsparcia nie może być mniejszy niż:
    - Uczenie modelu matematycznego w oparciu o widziany faktyczny ruch REST API
    - Budowanie automatyczne schematu struktury API w oparciu o obserwowany ruch
    - Ruch niezgodny z wyuczonym profilem uznawany jest za atak
28. Oferowany system musi obsługiwać ochronę komunikacji API w trybie Gateway. Oczekiwane funkcje w tym trybie to co najmniej:
    - zarządzanie użytkownikami (API user management),
    - weryfikacja kluczy dostępowych (API keyverification),
    - kontrola dostępu (API accesscontrol),
    - ograniczanie prędkości komunikacji (Rate limit control),
    - zmiana wywołań API (API callrewriting).
29. System ochrony aplikacji musi być wyposażony w mechanizm wykrywania komunikacji pochodzącej od internetowych bot’ów. Wykrywanie musi być oparte co najmniej o następujące mechanizmy:
    - Reputacja adresów IP
    - Sygnatury
    - Wartości progowe generowanego ruchu
    - Uczenie maszynowe: powinno działać w trybie nauki modelu matematycznego standardowego zachowania użytkowników. Po zebraniu informacji system powinien przejść do trybu ochrony, gdzie wykrycie zachowania odbiegającego od normy powinno skutkować uznaniem źródła za automat.

Wymagane funkcje dodatkowe

1. Kontrola antywirusowa dla komunikacji HTTP realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół ICAP. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.
2. System ochrony musi posiadać własny, wbudowany skaner podatności aplikacji www lub możliwość integracji z komercyjnymi skanerami firm trzecich. Skaner musi mieć możliwość wykonywania skanów chronionej aplikacji oraz w oparciu o wynik przygotować rekomendacje zmiany konfiguracji profili ochrony. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje, support) niezbędne do uruchomienia tej funkcjonalności. Zakres skanowania musi obejmować co najmniej:
   - Podatności związane z typowymi atakami jak na przykład Blind SQL Injection; BufferOverflow Attack; CORS Origin; CSRF, Cross Site Scripting, SQL Injection itd.
   - Ataki Brute Force co najmniej dla uwierzytelnienia podstawowego oraz w postaci formularza HTML
   - Nawigacja po aplikacji (crawl) i wykrywanie elementów niosących ryzyko bezpieczeństwa,
   - Pobranie charkterystycznych informacji o aplikacji, przykładowo: Cookies, Empty Body, Code Disclosure, Credit Card Numbers, Cross Domain Javascrip, Content Security Policy Headers, Error 500 Pages, Error Pages, Email Address Found, Hashes Identification, Analyze HTML Comments, Session ID in URL, Websockets Links Found.
   - Możliwości rozpoznania systemów I narzędzi wykorzystanych do budowy aplikacji, np Virtual Hosts, Web Application Firewall Identification, Operating System Identification, Frontpage Version Identification, HTTP Load Balancers Found, Server Identification, PHP Version Identification, Server Type Identification.
   - W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje) niezbędne do uruchomienia tej funkcji dla nielimitowanej ilości skanowanych aplikacji.
3. Ochrona przed wyciekiem informacji (DLP) realizowana na firewall'u aplikacyjnym lub zewnętrznym systemie w oparciu o protokół ICAP. W ramach postępowania muszą zostać dostarczone wszystkie elementy (urządzenia, licencje, support) niezbędne do uruchomienia tej funkcjonalności, która musi obejmować co najmniej:
   - Tworzenie własnych reguł, słowników i wzorców
   - Tworzenie wzorców powinno bazować na słowach kluczowych, wyrażeniach regularnych oraz wartościach hexadecymalnych
4. Dekodowanie Base64 oraz CSS.
5. Uwierzytelnianie użytkowników w oparciu o protokół SAML.
6. Rozpoznawanie i możliwość śledzenia prawidłowo zalogowanych użytkowników do chronionej aplikacji (User Tracking).
7. Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji.
8. Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa.
9. Możliwość uruchomienia AD FS Proxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day.
10. Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych/weryfikacji behawioralnej.
11. Cross-Origin Resource Sharing (CORS) protection.
12. Integracja z Lets's encrypt pozwalająca na automatyczne generowanie certyfikatów.

Zarządzanie

1. Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API.

2. Urządzenie musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach. Uwierzytelnianie administratorów musi się odbywać za pomocą lokalnej bazy urządzenia oraz serwera RADIUS lub TACACS+.
3. Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture.
4. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
5. Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych.
6. System musi udostępniać interfejs REST API do automatyzacji pracy z systemem. Poprzez API musi być możliwe odczytywanie konfiguracji, jej zmiana oraz monitorowanie. Producent musi dostarczyć dokumentację działania REST API wraz z przykładami.

Logowanie i Raportowanie

1. System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów.
2. Możliwość logowania do zewnętrznego serwera syslog i SIEM.
3. Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.
4. Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.
5. Możliwość maskowania w logach pól wrażliwych

Sygnatury, subskrypcje

1. Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.
2. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
    - Kontrolę antywirusową, sygnatury ochrony dla aplikacji www, bazy reputacyjne adresów IP na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
2. W ramach wsparcia wymagany jest do dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
3. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim przez producenta lub autoryzowanego polskiego partnera serwisowego.
4. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży na terenie Unii Europejskiej.

Szkolenie

Wymagane jest przeprowadzenie szkolenia z zakresu podstawowej konfiguracji i zarządzania urządzeniem przez wykonawcę lub autoryzowanego polskiego partnera serwisowego. Dopuszcza się szkolenie w formie videokonferencji. Szkolenie należy przeprowadzić najpóźniej 14 dni od dnia dostarczenia urządzeń.