**DZP.381.59A.2022 Zmodyfikowany załącznik nr 6**

***(załącznik nr 2 do umowy)***

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Minimalne wymagania dla systemu ochrony aplikacji webowych

|  |  |
| --- | --- |
| ***Lp.*** | ***Opis parametrów*** |
| 1 | Infrastruktura Zamawiającego |
|  | Zamawiający obecnie posiada urządzenie FortiWeb-400C produkcji Fortinet bez aktualnego wsparcia.  Zamawiający wymaga aby dostarczone środowisko zostało skonfigurowane zgodnie z obecnie zastosowanymi politykami.  Zamawiający dopuszcza dostawę w postaci środowiska wirtualnego do uruchomienia w posiadanym przez Zamawiającego środowisku VMware |
| 2 | Wymagania ogólne |
|  | System ochrony aplikacji webowych oraz Firewall XML, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w aplikacje webowe a następnie alarmowanie w wyniku wystąpienia określonych zdarzeń. |
|  | W ramach postępowania muszą zostać dostarczone wszystkie elementy systemu niezbędne do uruchomienia wymaganych funkcjonalności |
| 3 | Architektura systemu |
|  | Dla zapewnienia bezpieczeństwa funkcjonowania dostarczonego systemu oraz  szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie były certyfikowane przez producenta dostarczonego rozwiązania. |
| 4 | System operacyjny |
|  | Dla zapewnienia wysokiej sprawności i skuteczności działania systemu musi on pracować w oparciu o dedykowany system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu. |
| 5 | Wsparcie dla infrastruktury |
|  | Wsparcie przynajmniej dla systemów wirtualizacyjnych tj. dla: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w w/w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny. |
| 6 | Licencjonowanie |
|  | Licencjonowanie bez limitu chronionych serwerów, domen, aplikacji web (licencja na system). |
| 7 | Tryb działania |
|  | Możliwość implementacji systemu w trybach Reverse-Proxy lub Transparentnym. |
| 8 | Parametry wydajnościowe |
|  | Przepustowość dla ruchu HTTP – co najmniej 100 Mbps |
| 9 | Pozostałe parametry |
|  | Obsługuje minimum 2 wirtualne procesory.  Obsługuje nie mniej niż 4 interfejsy typu 10/100/1000 Mbps.  Obsługuje nie mniej niż 1TB z możliwością powiększenie do minimum 2TB. |
| 10 | Tryb wysokiej dostępności |
|  | W celu zwiększenia niezawodności system należy dostarczyć i skonfigurować do pracy w konfiguracji HA (High Availability) z trybem Active-Passive i Active-Active. |
| 11 | Logowanie i raportowanie |
|  | Lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów.  Funkcjonalność wysyłania logów do serwera typu syslog i SIEM.  Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem.  Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.  Funkcjonalność wysyłania logów do systemu FortiAnalyzer (produkcji Fortinet) będącego w posiadaniu Zamawiającego. |
| 12 | Zarządzanie |
|  | Interfejs zarządzający dostępny poprzez protokół HTTPS, SSH, API.  Dostęp do panelu administratora tylko dla zaufanych adresów IP.  Funkcjonalność wykonywania kopii bezpieczeństwa konfiguracji na zdalny serwer.  Możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. |
| 13 | Diagnostyka |
|  | Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture. |
| 14 | Testy bezpieczeństwa |
|  | Wykonawca do dostawy dołączy wyniki testów bezpieczeństwa oferowanego rozwiązania.  pochodzących od niezależnych organizacji takich jak: NSS Labs, ICSA Labs lub innych zajmujących się testowaniem tego rodzaju systemów |
| 15 | Sygnatury, subskrypcje |
|  | Bazy sygnatur wykorzystywane przez funkcje ochronne powinny być systematycznie aktualizowane zgodnie ze zdefiniowanych harmonogramem.  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 oraz bazy reputacyjne adresów IP na okres 36 miesięcy. |
| 16 | Wymagane funkcjonalności podstawowe |
| A | System musi realizować co najmniej poniższe funkcje:   * Obsługa protokołów: - http 1.1, http 2.0, FTP. * 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 Domain Hash * Wsparcie dla mechanizmów session persistence: * Source IP * HTTP Header * URL parameter * Insert Cookie * Rewrite Cookie * Persistent Cookie * Embedded Cookie * ASP Session ID * PHP Session ID * JSP Session ID * SSL Session ID * Terminowanie połączeń SSL dla wybranych chronionych serwisów. Wsparcie dla TLS 1.1, TLS 1.2. TLS 1.3. * Możliwość analizy ruchu do aplikacji po protokołach HTTP/HTTPS w oparciu o zaimplementowane polityki bezpieczeństwa. * 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. * DoS w warstwie aplikacji. * Ochrona przed atakami typu Brute force. * Ochrona przed atakami clickjacking. * Ochrona przed credential stuffing. * Mechanizmy ochrony przed wyciekiem informacji poufnych. * Filtrowanie ruchu do aplikacji w oparciu o geo-lokalizację. * Analiza komunikacji w oparciu o bazy reputacyjne adresów IP, dostarczane przez producenta rozwiązania. * Możliwość integracji z zewnętrznymi systemami uwierzytelniania dwu-składnikowego. * Wsparcie dla ochrony HTTP/1.1 i HTTP/2 oraz offload dla HTTP/1.1 i HTTP/2 w trybie pracy reverse proxy. * Wsparcie dla ochrony cookie, w tym szyfrowania oraz sprawdzania flag „Secure" „ oraz „http only”. * Content routing na bazie parametrów http oraz certyfikatów X.509. * Ochrona przed Web Scraping. * Wsparcie dla kompresji danych oraz cache. * Publikacja aplikacji web oraz OWA z zastosowaniem single sign on (http basic, kerberos). * Wsparcie dla aplikacji wykorzystujących AJAX oraz JSON, XML, AMF3. * Ochrona przed atakami typu SLOW (Slowloris i podobne). * 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 * Funkcja korzystania ze źródłowego adresu IP przekazywanego w nagłówku http „X-Forwared-For”. * Wszelkie klucze prywatne zapisywane na dyskach muszą być zapisywane w postaci zaszyfrowanej. * Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka. * Ustawienie wymaganej sekwencji otwieranych stron. * Sprawdzanie pól w nagłówkach http oraz samym protokole. Sprawdzanie długości payload’u HTML. * Wsparcie dla walidacji OpenAPI, JSON i XML. * Blokowania „Illegal XML Format” oraz „Illegal JSON Format”. * Możliwość wysłania odszyfrowanego przez system ruchu do innego systemu celem dalszej analizy. * Przydzielanie różnych certyfikatów dla różnych nazw domenowych. * Ochrona przed atakami MiTB (Man-in-the-Browser) przynamniej dla Anti-keylogger, Obfuscate. * URL Encryption. |
| B | System musi posiadać możliwość automatycznego uczenia się działania aplikacji (AI-based Machine Learning) 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 * anomalie muszą być poddawane dedykowanej analizie bezpieczeństwa w innej technice niż pozostałe funkcje bezpieczeństwa systemu. Technika ta musi umożliwiać wykrywanie nieznanych wcześniej ataków, tzw zero-day. * logika uczenia maszynowego musi uwzględniać błędy użytkowników/klientów, które nie dotyczą bezpieczeństwa i będą przesyłane do serwera aplikacji celem ułatwienia obsługi takich sytuacji przez logikę zaszytą w aplikację * system automatycznie wykrywa zmiany po stronie aplikacji lub zachowania użytkowników i ponawia proces uczenia. Uruchomienie uczenia musi mieć możliwość działania nie rzadziej niż 20 minut od zakończenia poprzedniego cyklu * 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 |
| C | System musi posiadać funkcje ochrony komunikacji API wspieraną technologią uczenia maszynowego (Machine Learning based API Discovery and Protection). 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 |
| D | 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 key verification), * kontrola dostępu (API access control), * ograniczanie prędkości komunikacji (Rate limit control), * zmiana wywołań API (API call rewriting). |
| E | System ochrony aplikacji musi być wyposażony w mechanizm wykrywania komunikacji pochodzącej od internetowych bot’ów (Bot mitigation). Wykrywanie musi być oparte co najmniej o następujące mechanizmy:   * reputacja adresów IP * sygnatury * wartości progowe generowanego ruchu * monitorowanie biometryczne – obserwowanie zdarzeń związanych z ruchem myszy, klikiem myszy, zdarzeń klawiatury, przewijania, sterowania dotykiem * rozpoznawanie przez umieszczenie niewidocznego na stronie linku url (bot deception). Otwarcie linku powoduje uznanie źródła za automat * 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. |
| F | System ochrony musi posiadać własny, wbudowany skaner podatności aplikacji www, który ma możliwość wykonywania skanów chronionej aplikacji oraz w oparciu o wynik przygotować rekomendacje zmiany konfiguracji profili ochrony. Zakres skanowania musi obejmować co najmniej:   * podatności związane z typowymi atakami jak na przykład Blind SQL Injection;  Buffer Overflow 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 charketrystycznych 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. |
| G | Oferowany system musi posiadać możliwość integracji z zewnętrznymi skanerami aplikacji. Oczekiwane możliwości integracji z produktami: Acunetix, IBM AppScan, WhiteHat, HP WebInspect, Qualys, Telefonica FAAST, ImmuniWEB. Integracja musi polegać na co najmniej importowaniu wyniku skanu do systemu ochrony aplikacji oraz automatyczne przygotowanie rekomendacji konfiguracji polityk na podstawie zawartości raportu importowanego skanowania. |
| H | Wymagana jest bezpośrednia integracja z posiadanym przez Zamawiającego sprzętowym firewallem, aby możliwe było pobieranie okresowe adresów IP, które są poddane kwarantannie po stronie firewall’a i automatycznie włączenie ich do ochrony aplikacji poprzez blokowanie ruchu z podejrzanego źródła. Blokada musi być realizowana zamiennie bezpośrednio na adresie IP źródłowym lub adresie IP pochodzącym z nagłówka X-Forwarded-For. |
| I | System ochrony aplikacji musi wspierać integrację bezpośrednio z co najmniej jednym typem systemu ochrony sandbox w wersji on-premise (fizyczny appliance lub maszyna wirtualna). Integracja musi być standardową funkcją, wspieraną przez producenta. Zakres integracji musi być nie mniejszy niż:   * automatyczne wysyłanie plików do analizy, * w wypadku, gdy sandbox zwróci ostrzeżenie o złośliwym pliku minimalne akcje jakie musi podjąć ochrona oferowanego systemu to:   + odpowiedni wpis w logach bezpieczeństwa,   + podjęcie akcji definiowanej w regułach bezpieczeństwa: alarm, alarm i blokada, blokada   + integracja z FortiGate w zakresie wspólnych baz IP |
| 17 | Wymagane funkcjonalności dodatkowe |
|  | * 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 systemu 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. * Skaner aplikacji WWW realizowany bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie (w przypadku zewnętrznego systemu skanującego – musi istnieć możliwość importu wyników skanowania do systemu WAF oraz na tej podstawie konfiguracji polityk ochrony). W ramach postępowania muszą zostać dostarczone wszystkie elementy systemu niezbędne do uruchomienia tej funkcji. * Ochrona przed podmianą strony WWW realizowana bezpośrednio na firewall’u aplikacyjnym lub zewnętrznym systemie. W ramach postępowania muszą zostać dostarczone wszystkie elementy systemu niezbędne do uruchomienia tej funkcji. * Dekodowanie Base64 oraz CSS. * Domyślne szablony ochrony dla Exchange, SharePoint i WordPress. * Uwierzytelnianie użytkowników w oparciu o protokół SAML. * Rozpoznawanie prawidłowo zalogowanych użytkowników do chronionej aplikacji. * Wsparcie dla CAPTCHA i Real Browser Enforcement do weryfikacji użytkowników. * Budowa rankingu punktowego lub określanie poziomu zagrożenia dla ruchu z możliwością określenia progów dla poszczególnych akcji: logowanie, blokowanie, kwarantanna czasowa. * Możliwość uruchomienia ADFSProxy oraz stworzenia polityki w celu sprawdzania ruchu do serwerów ADFS, ich ochrony pod kątem malware, botów, exploitów, oraz ataków DoS, APT i zero day. * Możliwość znakowania przez administratorów systemu za pomocą znaczników (flag) lub komentarza zdarzeń zalogowanych przez system w celu późniejszej ich analizy. * Ochrona przed botami dla: strony internetowej, aplikacji mobilnej, intefejsu API - przy zastosowaniu funkcji biometrycznych. * Cross-Origin Resource Sharing (CORS) protection. |
| 18 | Wdrożenie |
|  | Zamawiający wymaga aby realizacja niniejszego zadania została przeprowadzona przez personel posiadający aktualne certyfikaty techniczne producenta lub autoryzowanego dystrybutora w zakresie zarządzania i konfiguracji dostarczanego rozwiązania. |
| 19 | Szkolenia |
|  | Zamawiający wymaga przeszkolenia minimum 2 pracowników Zamawiającego z dostarczonego rozwiązania przez wykwalifikowany personel Wykonawcy potwierdzone certyfikatem. |
| 20 | Gwarancja (kryterium oceny ofert) |
|  | Wykonawca udzieli gwarancji na dostarczony przedmiot zamówienia na okres min 36 miesięcy od daty podpisania protokołu końcowego odbioru zgodnie z okresem zadeklarowanym w formularzu ofertowym.  W ramach gwarancji Wykonawca zapewni:   * Asystę techniczną producenta lub autoryzowanego dystrybutora * Wsparcie techniczne Wykonawcy * Bieżąca, systematyczna aktualizacja baz sygnatur wykorzystywanych przez funkcje ochronne. Aktualizacja musi obejmować: kontrolę antywirusową, sygnatury ochrony dla aplikacji www oraz bazy reputacyjne adresów IP |
| 21 | Asysta techniczna producenta lub autoryzowanego dystrybutora |
|  | Warunki świadczenia Asysty technicznej producenta lub autoryzowanego dystrybutora:   * świadczona w trybie 24/7 (24 godziny przez 7 dni w tygodniu) * świadczona w języku polskim * zapewnienie kontaktu telefonicznego z pomocą techniczną * czat internetowy w celu uzyskania szybkich odpowiedzi * portal wsparcia do tworzenia zgłoszeń * dostęp do aktualizacji oprogramowania.   Czasy reakcji na zgłaszane błędy:   * czas reakcji w przypadku błędu krytycznego 1 godzina od momentu zgłoszenia błędu przez Zamawiającego * czas reakcji w przypadku pozostałych błędów 1 dzień od momentu zgłoszenia błędu przez Zamawiającego   Czasy usunięcia błędów:   * dla błędu krytycznego - 4 godziny od momentu zgłoszenia błędu przez Zamawiającego * dla błędów pozostałych - 2 dni od momentu zgłoszenia błędu przez Zamawiającego   Błąd krytyczny – błąd uniemożliwiający użytkowanie dostarczonego rozwiązania (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika i prowadzący do zatrzymania jego eksploatacji).  Pozostałe błędy – błędy nie będące błędami krytycznymi czyli stan mający wpływ na poprawne funkcjonowanie dostarczonego rozwiązania lub jego składowych, odbiegający od założeń, niezakłócający rutynowej eksploatacji rozwiązania. |
| 22 | Wsparcie techniczne Wykonawcy (kryterium oceny ofert) |
|  | * Wsparcie techniczne Wykonawcy świadczone w języku polskim obejmuje: * udzielanie pomocy dotyczącej obsługi, konfiguracji, optymalizacji i administracji dostarczonym rozwiązaniem * udzielanie pomocy dotyczącej bieżącej obsługi dostarczonego rozwiązania * diagnozowanie problemów dotyczących funkcjonowania dostarczonego rozwiązania   Usługi wsparcia technicznego będą świadczone w wybranej przez Wykonawcę formule:   * + 1. w trybie 8 godzin przez 5 dni w tygodniu tj. w godzinach pracy Zamawiającego (od 7:00 do 15:00) przez 5 dni w tygodniu (8 godzin dziennie liczonych od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy) z czasem uzyskania pomocy max 8 godzin roboczych od momentu zgłoszenia przez Zamawiającego, realizowane telefonicznie, za pośrednictwem e-mail lub za pomocą sesji zdalnych   lub  b) w trybie 24 godzin przez 7 dni w tygodniu tj. w godzinach od 07:00-07:00 - 24 godziny dziennie przez 7 dni w tygodniu z czasem uzyskania pomocy max 8 godzin od momentu zgłoszenia przez Zamawiającego, realizowane telefonicznie, za pośrednictwem e-mail lub za pomocą sesji zdalnych  Wykonawca w formularzu ofertowym wskazuje, którą formułę wsparcia serwisowego (a lub b) deklaruje. |