|  |  |  |  |
| --- | --- | --- | --- |
| **LP.** | **Nazwa elementu, parametru lub cechy** | **Szczegółowy opis wymagań** | **Potwierdzenie zgodności parametrów\*** |
| **1** | **2** | **3** | **4** |
| **1.** | Web Application Firewall | | |
| 1.1. | **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. Powinien zostać dostarczony w postaci komercyjnej platformy instalowanej w środowisku wirtualnym: VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, KVM, Amazon Web Services (AWS) and Microsoft Azure, Google Cloud, Oracle Cloud. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych w ww środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić niezbędny odpowiednio zabezpieczony systemem operacyjny. |  |
| 1.2. | **Architektura systemu** | * Dla zapewnienia wysokiej sprawności i skuteczności działania wymaganym jest aby elementy systemu pracowały w oparciu o dedykowane oprogramowanie, wzmocnione z punktu widzenia bezpieczeństwa. * Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje podstawowe oraz zastosowane w nich technologie pochodziły od jednego producenta. Nie dopuszcza się aby elementy funkcji podstawowych zastosowanych w systemie były opracowane przez firmy trzecie. * Musi istnieć możliwość implementacji systemu w trybach: inline reverse proxy lub transparent. * Produkt nie może posiadać ograniczeń co do ilości chronionych aplikacji web. * Powinna istnieć możliwość zdefiniowania co najmniej 4 domen administracyjnych, w których poszczególni administratorzy zarządzają określonymi funkcjami podstawowymi systemu. * System powinien mieć możliwość pracy w konfiguracji HA (High Availability) w trybie Active-Passive i Active-Active. |  |
| 1.3. | **Parametry fizyczne systemu** | * System realizujący funkcje podstawowe musi obsługiwać minimum:   + 4 interfejsy sieciowe   + Ilość wirtualnych procesorów: 2 * Obługa powierzchni dyskowej - minimum 1 TB. |  |
| 1.4. | **Parametry wydajnościowe** | * Przepustowość dla ruchu http - min 100 Mbps. |  |
| 1.5. | **Podstawowe funkcje systemu** | System musi realizować co najmniej poniższe funkcje:   * Obsługa protokołów: - http 1.1, http 2.0, FTP. * Automatyczne tworzenie profili ochronnych aplikacji na bazie zaobserwowanego ruchu. Możliwość wyboru trybu wymuszania wyuczonego schematu bez konieczności akceptacji przez administratora. * Automatyczne tworzenie profilu ochrony przed botami na bazie zaobserwowanego ruchu użytkowników * Podział obciążenia na kilkanaście serwerów (loadbalancing) z mechanizmami weryfikacji stanu pracy serwerów. Wsparcie dla mechanizmów podziału obciążenia: * Round Robin, * Weighted Round Robin, * Least Connection, * 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. * 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. * Integracja 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 urządzenia muszą być zapisywane w postaci zaszyfrowanej.   + Możliwość konfigurowania własnych stron z informacjami o błędzie per polityka.   + 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. |  |
| 1.6. | **Wymagane funkcje 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 (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. * 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 (urządzenia, licencje) 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 (urządzenia, licencje) 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 akcji: 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 urządzenie 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. * Integracja z Let’s encrypt pozwalająca na automatyczne generowanie certyfikatów na potrzeby terminowania połączeń SSL. |  |
| 1.7. | **Zarządzanie** | * Dostarczony system musi umożliwiać lokalne zarządzanie z wykorzystaniem protokołów HTTPS, SSH, API. * Element systemu pełniący funkcję Web Application Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: packet capture. * Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych. * Możliwość przechowywania lokalnie na urządzeniu do 10 plików konfiguracyjnych. |  |
| 1.8. | **Logowanie i Raportowanie** | * System musi zapewniać lokalne logowanie oraz raportowanie - w oparciu o zestaw predefiniowanych wzorców raportów. * Możliwość logowania do zewnętrznego serwera syslog i SIEM. * Obsługa powiadomień o zdarzeniach systemowych oraz incydentach bezpieczeństwa mailem. * Powiadomienia o zdarzeniach systemowych oraz incydentach bezpieczeństwa za pośrednictwem trapów SNMP.. |  |
| 1.9. | **Certyfikaty** | * Z punktu widzenia jakości i skuteczności rozwiązania koniecznym jest przedstawienie wyników testów niezależnych organizacji, np. NSS Labs, ICSA Labs lub równoważnego. |  |
| 1.10. | **Sygnatury, subskrypcje** | * System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. * 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. |  |
| 1.11. | **Gwarancja oraz wsparcie** | * System musi być objęty serwisem producenta przez okres 24/36 miesięcy (zgodnie z deklaracja w polu kolumny 4)   **24 miesięcy = 0 pkt.**  **36 miesięcy =40 pkt.**   * W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. | Podać: |
| 2. | Centralny system logowania | | |
| 2.1. | **Wymagania ogólne** | * W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. * Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP). |  |
| 2.2. | **Interfejsy, Dysk** | * System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 3 TB. |  |
| 2.3. | **Parametry wydajnościowe** | * System musi być w stanie przyjmować minimum 10 GB logów na dzień. * Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów. |  |
| **W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:** | | | |
| 2.4. | **Logowanie** | * Podgląd logowanych zdarzeń w czasie rzeczywistym. * Możliwość przeglądania logów historycznych z funkcją filtrowania. * System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: * Listę najczęściej wykrywanych ataków. * Listę najbardziej aktywnych użytkowników. * Listę najczęściej wykorzystywanych aplikacji. * Listę najczęściej odwiedzanych stron www. * Listę krajów , do których nawiązywane są połączenia. * Listę najczęściej wykorzystywanych polityk Firewall. * Informacje o realizowanych połączeniach IPSec. * Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. * Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. * System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy. |  |
| 2.5. | **Raportowanie** | * Generowanie raportów co najmniej w formatach: PDF, CSV. * Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. * Funkcję definiowania własnych raportów. * Możliwość spolszczenia raportów. * Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email. |  |
| 2.6 | **Korelacja logów** | * Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. * Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. * Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: * Malware. * Aplikacje sieciowe. * Email. * IPS. * Traffic. * Systemowe: utracone połączenie vpn, utracone połączenie sieciowe. * Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań |  |
| 2.6 | **Zarządzanie** | * System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. * Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. * System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi. |  |
| 2.7 | **Serwisy i licencje** | * System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania. * Wsparcie: System musi być objęty serwisem producenta przez okres 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
| 2.8 | **Wymagania podstawowe** | * Obsługa minimum 8 urządzeń sieciowych z możliwością rozbudowy do 1000 urządzeń. * Wymagana jest architektura serwer-klient z dostępem do systemu poprzez przeglądarkę WWW (Google Chrome 85, Firefox 80, Microsoft Edge 89 lub nowsze) * Wymagany interfejs użytkownika w języku polskim lub angielskim * Obsługiwana lokalna baza użytkowników systemu * Czasowe blokowanie możliwości logowania użytkownika systemu w przypadku 5-krotnego podania błędnego hasła * W przypadku gdy oprogramowanie korzysta z systemu licencjonowania powinna być zapewniona możliwość sprawdzenia zainstalowanej licencji oraz zmiany licencji * Monitorowanie wykorzystania licencji i informowanie użytkownika systemu o zbliżającej się dacie wygasania licencji, bądź przekroczenia limitów zainstalowanej licencji (np. Ilość obsługiwanych urządzeń) * Dostępna w systemie zarządzającym dokumentacja w języku polskim lub angielskim. * Wraz z systemem zarządzania należy dostarczyć dedykowany serwer fizyczny. |  |
| 2.9. | **Zarządzenie alertami** | * Możliwość automatycznego alarmowania opartego o zadane progi alarmowe, w tym * możliwość definiowania dwóch progów – ostrzegawczy i alarmowy * Możliwość automatycznego alarmowania opartego o profil ruchu * Możliwość automatycznego alarmowania o przekroczeniu obciążenia interfejsu z uwzględnienie dwóch progów - ostrzegawczy i alarmowy * Możliwość określenia listy osób i grup osób powiadamianych przy poszczególnych * Możliwość wykorzystania następujących kanałów powiadomienia dla poszczególnych poziomów alarmów   + konsola operatora   + e-mail |  |
| 2.10. | **Monitorowanie** | * Możliwość monitorowania zdarzeń związanych z funkcjonowaniem monitorowanych urządzeń w czasie rzeczywistym (CPU, pamięć) * Możliwość monitorowania urządzeń sieciowych oraz ruchu sieciowego w oparciu o protokóły SNMP * Możliwość zbierania danych z urządzeń firm trzecich generowanych w oparciu o protokół SNMP * Możliwość zapisywania niezagregowanych danych pochodzących z monitorowanych urządzeń przez okres 30 dni. * Możliwość archiwizacji dostępnych danych niezagregowanych. * Możliwość monitorowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem   + Wartości aktualnych   + Wartości szczytowych * Możliwość pozyskania informacji o statusie monitorowanych urządzeń sieciowych * Możliwość pozyskania informacji o statusie portu * Możliwość ręcznego definiowania progów czułości alarmów * Możliwość przesyłania powiadomień o alarmach za pomocą mechanizmu SNMP trap * Możliwość monitorowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem rozgraniczenia dla ruchu wchodzącego i wychodzącego * Możliwość wyświetlania 95 percentyla dla raportów obciążenia interfejsów niezależnie dla kierunku wejściowego i wyjściowego |  |
| 2.11. | Zarządzanie konfiguracją | * Możliwość współpracy z urządzeniami sieciowymi różnych producentów * Wsparcie dla protokołu SNMP (wersja 1,2,3) * Możliwość konfigurowania zarządzanych urządzeń sieciowych * Możliwość automatycznego wykrywania urządzeń sieciowych * Możliwość automatycznego odczytywania z monitorowanych i zarządzanych urządzeń ich nazw, listy interfejsów wraz z ich nazwami i prędkościami. System zarządzania i monitorowania sieci powinien umożliwiać dokonywanie automatycznego odczytu o zdefiniowanej g * Możliwość stworzenia mapy topologii fizycznej i logicznej sieci * Możliwość tworzenia i zarządzania sieciami VLAN (niezależnie od fizycznej lokalizacji urządzeń) * Możliwość pełnego dostępu i zarządzania systemem monitorowania i zarządzania siecią zarówno lokalnie jak i zdalnie * Możliwość uzyskania zdalnego dostępu do urządzeń sieciowych i dokonania zmian w ich konfiguracji. * Możliwość definiowania w systemie monitorowania i zarządzania siecią użytkowników z nadawaniem uprawnień na poziomie poszczególnych urządzeń oraz grupy urządzeń, do odczytu konfiguracji urządzenia, zarządzania urządzeniem. * Możliwość stworzenia kopii zapasowej ustawień urządzeń * Możliwość przywrócenia kopii zapasowej ustawień urządzeń * Możliwość ręcznego dodawania opisów do poszczególnych interfejsów monitorowanych urządzeń * Możliwość logowania i uwierzytelniania w oparciu o lokalną bazę użytkowników * Możliwość wymuszenia logowania się wszystkich użytkowników systemu monitorowania i zarządzania siecią. * Możliwość przeprowadzenia testów dostępności urządzenia * Liczby przeprowadzonych udanych oraz nieudanych odpytań SNMP * Możliwość tworzenia szablonów konfiguracji dla danego modelu urządzenia * Możliwość zarządzania siecią WLAN, w tym kontrolerami sieci WLAN AC oraz punktami dostępowymi FIT/FAT AP. * Możliwość autentykacji urządzeń sieciowych w oparciu o protokół 802.1x (NAC) |  |
| 2.12 | **Raportowanie** | * Możliwość raportowania na poziomie pojedynczego urządzenia oraz grupy urządzeń obejmującego dostępne w Systemie - parametry sieciowe i wydajnościowe * Możliwość raportowania zdarzeń w trybie rzeczywistym - czasie zbliżonym do rzeczywistego, dla urządzeń * Możliwość raportowania w formie graficznej (wykresy) jak i tekstowej (tabela z wszystkimi konwersacjami) * Możliwość raportowania obciążenia całkowitego urządzeń oraz ich interfejsów z zachowaniem   + Wartości aktualnych   + Wartości szczytowych * Możliwość tworzenia raportów dostępności urządzeń * Możliwość przeglądania raportów za pośrednictwem przeglądarki WWW * Możliwość eksportu raportów do plików płaskich lub ustrukturyzowanych * Możliwość automatycznego generowania, zapisywania i wysyłania raportów pocztą email |  |
| 2.13 | **Administracja systemem i Bezpieczeństwo** | * Możliwość tworzenia unikalnych kont użytkowników * Możliwość zabezpieczenia Dostępu do kont użytkowników przy pomocy haseł * Możliwość logowania zdarzeń i aktywności użytkowników narzędzia * Możliwość zarządzania uprawnieniami na poziomie grup - pojedynczych użytkowników * Możliwość przypisywania użytkownikom - grupom uprawnień na poziomie czynności elementów konfiguracji (np. urządzenie sieciowe, grupa urządzeń sieciowych) * Możliwość definiowania wielu użytkowników, w tym możliwość różnicowania uprawnień odczytu oraz różnicowania uprawnień administracyjnych z podziałem na grupy urządzeń * Możliwość tworzenia widoków dla użytkowników w zależności od zakresu uprawnień * Możliwość tworzenia widoków jedynie do podglądu * Możliwość archiwizacji i odtwarzania danych narzędzia, w tym konfiguracji oraz informacji o licencji * Możliwość importu całej lub fragmentu konfiguracji narzędzia * Możliwość konfigurowania, zarządzania oraz monitorowania usług VPN (IPSec) |  |
| 2.14 | **Serwis gwarancyjny** | * Wymagany jest serwis gwarancyjny świadczony przez minimum 5 lat. * Dostępność serwisu 8x5xNBD * Rozwiązywanie problemów ze sprzętem i oprogramowaniem * Gwarantowany czas naprawy platformy sprzętowej aplikacji – 48h od momentu zgłoszenia * Dostęp do poprawek i nowych wersji oprogramowania w okresie serwisu. |  |

**\*należy wypełnić pola kolumny 4 - *Potwierdzenie zgodności parametró*w.**

**Wykonawca zobowiązany jest do wypełnienia każdego pola w kolumnie 4 tabeli poprzez wpis TAK lub NIE (potwierdza lub nie potwierdza zgodność parametrów oferowanego przedmiotu zamówienia z określonymi w odpowiednim polu w kolumnach 2 i 3)**

.........................................................

*(miejscowość, data)*

..........................................................

*(Dokument należy złożyć w postaci elektronicznej opatrzony*

*kwalifikowanym podpisem elektronicznym,*

*podpisem zaufanym lub podpisem osobistym)*