ŁABOWA 12.01.2022 r.

ODPOWIEDZI NA PYTANIA I MODYFIKACJA SWZ

nr postępowania: RI.271.3.17.2021

„WDROŻENIE E-USŁUG DLA MIESZKAŃCÓW GMINY ŁABOWA”

Na podst. art. 284 ust. 2 ustawy z dnia 11.09.2019r. Prawo zamówień publicznych (Dz. U. 2019 poz.2019 z późn. zm.) dalej PZP, Zamawiający informuje, że w niniejszym postępowaniu wpłynęły pytania odnoszące się do SWZ.

Pytanie nr 1:

Pytanie 1 – urządzenie UTM:
Wymagane przez Państwa rozwiązanie UTM jest wykorzystywane w organizacjach, urzędach powyżej 200 użytkowników. Z informacji uzyskanych u Państwa w urzędzie wynika, iż pracuje u Państwa około 50 użytkowników. W związku z kosztami zakupu i utrzymania urządzenia o cztery razy większego niż wymagana na dzień dzisiejszy liczba użytkowników koszt takiego urządzenia na dzień dzisiejszy kształtuje się na poziomie 60000 zł netto. W związku z chęcią złożenia oferty w Państwa postępowaniu mieszczącej się w Państwa budżecie projektu uprzejmie zwracamy się o obniżenie parametrów do urządzenia klasy premium dostosowanego do ponad 100 użytkowników. W związku z powyższym prosimy o zmianę wymagań UTMa na przedstawione poniżej jako rozwiązanie równoważne:
OBSŁUGA SIECI
1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP. ZAPORA KORPORACYJNA (Firewall)
2. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
3. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
4. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
5. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
6. Administrator musi mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia.
7. Rozwiązanie musi umożliwiać między innymi filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
8. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
9. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów).

10. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos). INTRUSION PREVENTION SYSTEM (IPS)
11. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
12. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
13. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
14. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
15. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej.
16. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.
17. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
18. Urządzenie ma mieć możliwość ochrony między innymi przed atakami typu SQL injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. KSZTAŁTOWANIE PASMA (Traffic Shapping)
19. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
20. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
21. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring).
22. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch. OCHRONA ANTYWIRUSOWA
23. Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
24. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
25. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
26. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia. OCHRONA ANTYSPAM
27. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).

28. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner.
29. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL.
30. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin. WIRTUALNE SIECI PRYWANTE (VPN)
31. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacjalokalizacja).
32. Odpowiednio kanały VPN można budować w oparciu o: a. PPTP VPN, b. IPSec VPN, c. SSL VPN.
33. SSL VPN musi działać w trybach Tunel i Portal.
34. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
35. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
36. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
37. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based. FILTR DOSTĘPU DO STRON WWW
38. Urządzenie ma posiadać wbudowany filtr URL.
39. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
40. Administrator musi mieć możliwość dodawania własnych kategorii URL.
41. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora.
42. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST.
43. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: a. blokowanie dostępu do adresu URL, b. zezwolenie na dostęp do adresu URL, c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
44. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
45. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.
46. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS.
47. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
48. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. UWIERZYTELNIANIE
49. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a. lokalną bazę użytkowników (wewnętrzny LDAP), b. zewnętrzną bazę użytkowników (zewnętrzny LDAP), c. usługę katalogową Microsoft Active Directory.
50. Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP.

51. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzacje w oparciu o protokoły: a. SSL, b. Radius, c. Kerberos.
52. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory.
53. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
54. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny. ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)
55. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
56. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a. równoważenie względem adresu źródłowego, b. równoważenie względem połączenia.
57. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
58. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
59. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów.
60. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
61. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP.
62. Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
63. Rozwiązanie powinno wspierać technologię Link Aggregation. POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA
64. Urządzenie musi posiadać wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci.
65. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay.
66. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6.
67. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS.
68. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3.
69. Urządzenie musi posiadać usługę DNS Proxy.
70. Urządzenie musi posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). ADMINISTRACJA URZĄDZENIEM
71. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
72. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.

73. Komunikacja może odbywać się na porcie innym niż https (443 TCP).
74. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
75. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana.
76. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https.
77. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS).
78. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX.
79. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora.
80. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
81. Urządzenie musi posiadać funkcjonalność anonimizacji logów. RAPORTOWANIE
82. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
83. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
84. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego.
85. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów.
86. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu.
87. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.
88. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy. PARAMETRY SPRZĘTOWE
89. Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 240 GB.
90. Liczba portów Ethernet 10/100/1000Mbps – min. 12.
91. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta.
92. Przepustowość Firewall – min. 8 Gbps.
93. Przepustowość Firewall wraz z włączonym systemem IPS – min. 3,3 Gbps.
94. Przepustowość filtrowania Antywirusowego – min. 950 Mbps.
95. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 1,3 Gbps.
96. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 500.
97. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 100.
98. Obsługa min. VLAN 256.
99. Liczba równoczesnych sesji - min. 500 000 i nie mniej niż 25 000 nowych sesji/sekundę.

100. Urządzenie musi dawać możliwość budowania klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
101. Urządzenie jest nielimitowane na użytkowników. Wymaga się, aby dostawa obejmowała również:
• Minimum 24-miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu.
• Licencje dla wszystkich funkcji bezpieczeństwa producentów na okres minimum 24 miesięcy liczoną od dnia zakończenia wdrożenia całego systemu.

Odpowiedź 1:
Mając na uwadze, że przedstawione propozycje obniżenia parametrów urządzenia UTM mają charakter istotny i znaczący dla wydajności i dostępności infrastruktury urzędu oraz fakt, że to Zamawiający określa swoje potrzeby Zamawiający nie wyraża zgody na obniżenie parametrów urządzenia UTM zgodnie z treścią przedmiotowego pytania. Dodatkowo należy zauważyć, że Zamawiający nie dokonuje oceny równoważności na etapie przed otwarciem ofert.

Pytanie nr 2:
„ Wyposażenie serwerowni - zakup UPS (1 szt.): Proszę o informację czy Zamawiający zaakceptuje jako urządzenie równoważne UPSa o parametrach:
1. Moc wyjściowa: min. 5 kVA
2. Architektura UPS: line interactive lub on-line.
3. Maks. czas przełączenia na baterię - 0 ms.
4. Ilość gniazd sieciowych: min. 6.
5. Porty: 1 x USB.
6. Typ obudowy – RACK.
7. Czas podtrzymania przy obciążeniu 100 % - min. 3 min.
8. Czas podtrzymania przy obciążeniu 50 % - min. 9 min.
9. Gwarancja producenta min. 24 miesiące.
Odpowiedź 2:
Mając na uwadze, że przedstawione propozycje obniżenia parametrów urządzenia UTM mają charakter istotny i znaczący dla wydajności i dostępności infrastruktury urzędu oraz fakt, że to Zamawiający określa swoje potrzeby Zamawiający nie wyraża zgody na obniżenie parametrów urządzenia UTM zgodnie z treścią przedmiotowego pytania. Dodatkowo należy zauważyć, że Zamawiający nie dokonuje oceny równoważności na etapie przed otwarciem ofert.

Pytanie nr 3:
Wyposażenie serwerowni - zakup urząd urządzenia UTM (1 szt.): Proszę o informację czy Zamawiający zaakceptuje jako urządzenie równoważne UTMa o parametrach: Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych,

komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego Strona 2 z 5 przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS.
System musi wspierać IPv4 oraz IPv6 w zakresie:
1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
Minimalne parametry techniczne urządzenia:
1. Przepustowość Firewall: min. 7 Gbps,
2. Musi obsługiwać min. 1 500 000 jednoczesnych połączeń.
3. Musi obsługiwać co najmniej 200 mobilnych połączeń VPN.
4. Automatyczna aktualizacja plików sygnatur antywirusowych.
5. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
6. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
7. Automatyczna aktualizacja sygnatur IPS.
8. IPS musi dokonać analizy warstwy aplikacji, a także mieć możliwość ustawienia poziomu nasilenia ataku, który ma generować zdalne alarmy.
9. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
10. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45. Interfejsy te powinny być skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
11. Wsparcie VLAN: Musi posiadać minimum 50 sieci VLAN.
12. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 950 Mbps. Strona 3 z 5
13. Administracja urządzenia musi być możliwe poprzez graficzny interfejs zarządzania.
14. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
− Kontrola dostępu
- zapora ogniowa klasy Stateful Inspection.
− Kontrola Aplikacji.
− Poufność transmisji danych
- połączenia szyfrowane IPSec VPN oraz SSL VPN.
− Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
− Ochrona przed atakami - Intrusion Prevention System.
− Kontrola stron WWW.
− Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

− Zarządzanie pasmem (QoS, Traffic shaping).
− Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
− Analiza ruchu szyfrowanego protokołem SSL. −
Analiza ruchu szyfrowanego protokołem SSH.
15. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
16. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
17. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
18. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
19. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
20. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach. Strona 4 z 5
21. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
22. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
23. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
24. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
25. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
26. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
27. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
28. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
29. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
30. Rozwiązanie powinno umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
32. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
33. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

34. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
35. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Strona 5 z 5
36. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
37. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
38. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenia.
39. Gwarancja producenta, min. 24 miesiące.
40. Zakres usług konfiguracyjnych:
W zakres usług konfiguracyjnych urządzenia UTM na styku z siecią Internet wedle wymagań Zamawiającego wchodzi: Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia; Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta, Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc.); Zamawiający wymaga migracji istniejących polityk z dotychczas wykorzystywanego urządzeń oraz ich modyfikacja po uzgodnieniu z Zamawiającym; Konfiguracja routingów statycznych na firewallu, Konfiguracja polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego, Konfiguracja filtracji stron WWW na podstawie kategorii oraz treści, Integracja UTMa z systemem autoryzacji Microsoft Active Directory tak aby możliwa była identyfikacja użytkowników, Konfiguracja dostępu zdalnego SSL VPN (VPN Client, portal WebVPN). Konfiguracja SSL Decryption łącznie z instalacją certyfikatów na stacjach klienckie np. przy użyciu funkcjonalności AD.

Odpowiedź 3:

Mając na uwadze, że przedstawione propozycje obniżenia parametrów urządzenia UTM mają charakter istotny i znaczący dla wydajności i dostępności infrastruktury urzędu oraz fakt, że to Zamawiający określa swoje potrzeby Zamawiający nie wyraża zgody na obniżenie parametrów urządzenia UTM zgodnie z treścią przedmiotowego pytania. Dodatkowo należy zauważyć, że Zamawiający nie dokonuje oceny równoważności na etapie przed otwarciem ofert.

Pytanie nr 4:

Podpunkt 1 Zakup licencji systemu e-zamówienia (1 szt.) - Podpunkt 18 i 38:

Czy Zamawiający uzna podpunkt 18 i 38 za spełniony w przypadku gdy dane wskazane w ramach punktu 18 za wyjątkiem wadium, raz wprowadzone będą mogły zasilić generowane formularze postępowania w ramach Platformy Zamówień Publicznych? W przypadku wadium, jego wartość jest zależna od przewidywanej wartości zamówienia, w związku z tym, czy Zamawiający zaakceptuje pole walidacji wadium w formularzu postępowania, które będzie informowało Zamawiającego o przekroczeniu wysokości wadium wskazanych w ustawie?

Odpowiedź 4:

Intencją Zamawiającego wyrażoną w punkcie 18 jest brak konieczności powielania wpisywania tych samych danych w obszarze postępowania, które mogą mu posłużyć w celu generowania różnych dokumentów dla tego postępowania. Zatem jeżeli raz wprowadzone do systemu wadium do postępowania będzie częścią dokumentu, który ma zostać wygenerowany w ramach postępowania to Zamawiający nie dopuszcza by pracownik Urzędu musiał w ramach tego postępowania wpisywać wartość wadium ponownie.

Pytanie nr 5:

Podpunkt 1 Zakup licencji systemu e-zamówienia (1 szt.) - Podpunkt 20:
Biorąc pod uwagę punkt 20 i bazując na doświadczeniu Wykonawcy w udostępnianiu usługi Platformy Zamówień Publicznych, korzystniejszym dla Zamawiającego rozwiązaniem jest prowadzenie postępowania i dokumentacji w jednym miejscu, czyli w ramach Platformy Zamówień Publicznych. Integracja z Biuletynem Informacji Publicznych Zamawiającego generuje dodatkowe koszty, i jest całkowicie zbędna, gdyż zgodnie z ustawą PZP, Zamawiający ma obowiązek prowadzenia postępowania publicznie w ramach jednej strony internetowej. Wycena takiej integracji mocno zwiększy koszty oferty, a rozwiązaniem optymalnym bezkosztowym jest załączanie na BIP informacji z linkiem o miejscu prowadzenia postępowania w ramach aplikacji PZP. Ponadto w Zamawiający ma obowiązek wskazania w ramach dokumentacji postępowania jednego miejsca prowadzenia tego postepowania, czyli Platformy Zamówień Publicznych. Prosimy o potwierdzenie, że Zamawiający w ramach tego postępowania nie wymaga integracji Platformy Zamówień Publicznych z Biuletynem Informacji Publicznych Zamawiającego. Jako rozwiązanie zastępcze proponujemy załączanie na BIPie informacji z linkiem o miejscu prowadzenia postępowania w ramach aplikacji PZP.

Odpowiedź 5:

Zamawiający informuje, że podtrzymuje funkcjonalność umożliwiającą integrację z BIP co najmniej w zakresie przekazywania do BIP z kupowanej platformy zamówień publicznych nazwy i linku postępowania.

Pytanie nr 6:

Dotyczy: Zakup urządzenia UTM (1 szt.):
Czy z uwagi na bardzo trudną sytuację na rynku polskim związaną z brakiem dostępności sprzętu teleinformatycznego i zachwianiem, a wręcz przerwaniem łańcuchów dostaw, spowodowanym trwającą pandemią koronawirusa Sars-Cov-2, Zamawiający potwierdzi interpretację Wykonawcy, iż urządzenie, które jest dostępne i możliwe do dostarczenia w

terminie oczekiwanym przez Zamawiającego o poniższych parametrach jest urządzeniem równoważnym do opisanego w Szczegółowym Opisie Przedmiotu Zamówienia:
System realizujący funkcję Firewall daje możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz hybrydowym.
System wspiera IPv4 w zakresie:
1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.
System wspiera IPv6.
Parametry techniczne urządzenia:
1. Przepustowość Firewall: min. 10 Gbps,
2. Obsługuje min. 1 500 000 jednoczesnych połączeń.
3. Obsługuje co najmniej 200 mobilnych połączeń VPN.
4. Automatyczna aktualizacja plików sygnatur antywirusowych.
5. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
6. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
7. Automatyczna aktualizacja sygnatur IPS.
8. IPS dokonuje analizy warstwy aplikacji, a także posiada możliwość ustawienia poziomu nasilenia ataku, który generuje zdalne alarmy.
9. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
10. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45 oraz 2 gniazda SFP+
11. Gbps. Interfejsy te są skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
12. Wsparcie VLAN: Posiada minimum 50 sieci VLAN.
13. Administracja urządzenia jest możliwa poprzez graficzny interfejs zarządzania.
14. System ochrony bezpieczeństwa realizuje wszystkie poniższe funkcje.
− Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
− Kontrola Aplikacji.
− Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
− Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
− Ochrona przed atakami - Intrusion Prevention System.
− Kontrola stron WWW.
− Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
− Zarządzanie pasmem (QoS, Traffic shaping).
− Analiza ruchu szyfrowanego protokołem SSL.
15. Producent rozwiązania dostarcza oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
16. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP
17. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

18. Istnieje możliwość określania pasma dla poszczególnych aplikacji.
19. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
20. System umożliwia skanowanie archiwów, w tym co najmniej: zip, RAR.
21. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
22. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Wraz z urządzeniem jest dostarczana platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
23. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
24. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
25. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
26. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
27. Administrator systemu posiada możliwość definiowania własnych wyjątków oraz własnych sygnatur.
28. Rozwiązanie umożliwia wysyłanie alarmów przez SNMP lub e-mail.
29. Urządzenie ma możliwość generowania raportów.
20. Elementy systemu bezpieczeństwa posiadają możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i posiadają możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
31. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
32. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
33. Element systemu pełniący funkcję Firewal posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
34. W ramach logowania system pełniący funkcję Firewall zapewnia przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Istnieje możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
35. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
36. Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Obejmują one następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenia.
37. Zakres usług konfiguracyjnych:
W zakres usług konfiguracyjnych urządzenia UTM na styku z siecią Internet wedle wymagań Zamawiającego wchodzi: Aktualizacja oprogramowania układowego do najnowszej stabilnej

wersji oferowanej przez producenta urządzenia; Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta, Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc.); Zamawiający wymaga migracji istniejących polityk z dotychczas wykorzystywanego urządzeń oraz ich modyfikacja po uzgodnieniu z Zamawiającym; Konfiguracja routingów statycznych na firewallu, Konfiguracja polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego, Konfiguracja filtracji stron WWW na podstawie kategorii oraz treści, Integracja UTMa z systemem autoryzacji Microsoft Active Directory tak aby możliwa była identyfikacja użytkowników, Konfiguracja dostępu zdalnego SSL VPN (VPN Client, portal WebVPN). Konfiguracja SSL Decryption łącznie z instalacją certyfikatów na stacjach klienckie np. przy użyciu funkcjonalności AD

Odpowiedź 6:

Zamawiający nie dokonuje oceny równoważności na etapie przed otwarciem ofert. Mając jednak na uwadze, że przedstawiona propozycja opisu przedmiotu zamówienia urządzenia UTM nie ma charakteru istotnego i nie prowadzi do obniżenia parametrów urządzenia UTM, Zamawiający informuje, że zmienia opis przedmiotu zamówienia dla urządzenia UTM nadając mu brzmienie:

System realizujący funkcję Firewall daje możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz hybrydowym.

System wspiera IPv4 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

System wspiera IPv6.

Parametry techniczne urządzenia:

1. Przepustowość Firewall: min. 10 Gbps,
2. Obsługuje min. 1 500 000 jednoczesnych połączeń.
3. Obsługuje co najmniej 200 mobilnych połączeń VPN.
4. Automatyczna aktualizacja plików sygnatur antywirusowych.
5. Skanowanie wszystkich plików skompresowanych (zip, tar, rar, gzip) z wieloma poziomami kompresji.
6. Możliwość wsparcia IPS z poziomu urządzenia poprzez dodatkowe subskrypcje.
7. Automatyczna aktualizacja sygnatur IPS.
8. IPS dokonuje analizy warstwy aplikacji, a także posiada możliwość ustawienia poziomu nasilenia ataku, który generuje zdalne alarmy.
9. Wsparcie dla wszystkich głównych protokołów: HTTP, FTP, SMTP, POP3.
10. Ilość interfejsów sieciowych: minimum 8 portów Gigabit Ethernet RJ-45 oraz 2 gniazda SFP+
11. Gbps. Interfejsy te są skonfigurowane jako jeden z trzech rodzajów wymaganych stref bezpieczeństwa.
12. Wsparcie VLAN: Posiada minimum 50 sieci VLAN.
13. Administracja urządzenia jest możliwa poprzez graficzny interfejs zarządzania.

14. System ochrony bezpieczeństwa realizuje wszystkie poniższe funkcje.
− Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
− Kontrola Aplikacji.
− Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
− Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS.
− Ochrona przed atakami - Intrusion Prevention System.
− Kontrola stron WWW.
− Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
− Zarządzanie pasmem (QoS, Traffic shaping).
− Analiza ruchu szyfrowanego protokołem SSL.
15. Producent rozwiązania dostarcza oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.
16. Zapewnienie obsługi Routingu statycznego, Policy Based Routingu, protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP
17. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
18. Istnieje możliwość określania pasma dla poszczególnych aplikacji.
19. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
20. System umożliwia skanowanie archiwów, w tym co najmniej: zip, RAR.
21. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
22. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Wraz z urządzeniem jest dostarczana platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
23. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
24. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
25. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
26. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
27. Administrator systemu posiada możliwość definiowania własnych wyjątków oraz własnych sygnatur.
28. Rozwiązanie umożliwia wysyłanie alarmów przez SNMP lub e-mail.
29. Urządzenie ma możliwość generowania raportów.
20. Elementy systemu bezpieczeństwa posiadają możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i posiadają możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
31. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

32. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
33. Element systemu pełniący funkcję Firewal posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
34. W ramach logowania system pełniący funkcję Firewall zapewnia przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Istnieje możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
35. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
36. Licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Obejmują one następujące elementy: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres gwarancji urządzenia.
37. Zakres usług konfiguracyjnych:
W zakres usług konfiguracyjnych urządzenia UTM na styku z siecią Internet wedle wymagań Zamawiającego wchodzi: Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia; Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta, Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email etc.); Zamawiający wymaga migracji istniejących polityk z dotychczas wykorzystywanego urządzeń oraz ich modyfikacja po uzgodnieniu z Zamawiającym; Konfiguracja routingów statycznych na firewallu, Konfiguracja polityki bezpieczeństwa (reguły dostępu dla ruchu z Internetu, do Internetu oraz między pozostałymi strefami) zgodnie z wytycznymi ze strony Zamawiającego, Konfiguracja filtracji stron WWW na podstawie kategorii oraz treści, Integracja UTMa z systemem autoryzacji Microsoft Active Directory tak aby możliwa była identyfikacja użytkowników, Konfiguracja dostępu zdalnego SSL VPN (VPN Client, portal WebVPN). Konfiguracja SSL Decryption łącznie z instalacją certyfikatów na stacjach klienckie np. przy użyciu funkcjonalności AD

Na podst. art. 286 ustawy z dnia 11.09.2019r. Prawo zamówień publicznych (Dz. U. 2019 poz.2019 z późn. zm.) Zamawiający modyfikuje zapisy SWZ, w sposób następujący:

1. **W miejsce zapisu w SWZ Rozdział IX pkt 7**
„ 7. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
8.1. akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
8.2. zapoznał i stosuje się do Instrukcji składania ofert dostępnej pod linkiem.
„***wprowadza się zapis:***
„ 7. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego: https://platformazakupowa.pl/strona/1-regulami

7.1. akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem : https://platformazakupowa.pl/strona/1-regulami

7.2. zapoznał i stosuje się do Instrukcji składania ofert dostępnej pod linkiem https://platformazakupowa.pl/strona/45-instrukcje

2. W miejsce zapisu w SWZ Rozdział IX pkt 24

„ 24. Osoba uprawnioną do kontaktu z Wykonawcami jest:

1.1. W zakresie procedury zamówienia:
Małgorzata Nowakowska – inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:mnowakowska@lanowa.pl
Małgorzata Kotlarska – inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:mk@lanowa.pl

1.2. W zakresie merytorycznym:
Przemysław Sulewski - inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:ps@lanowa.pl „

wprowadza się zapis:

„ 24. Osoba uprawnioną do kontaktu z Wykonawcami jest:

1.1. W zakresie procedury zamówienia:
Małgorzata Nowakowska – inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:mnowakowska@labowa.pl
Małgorzata Kotlarska – inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:mk@labowa.pl

1.2. W zakresie merytorycznym:
Przemysław Sulewski - inspektor Referat Inwestycji Urzędu Gminy Łabowa
e-mail:ps@labowa.pl „

3. W miejsce zapisu w SWZ Rozdział X

” **TERMIN ZWIĄZANIA OFERTĄ**

Wykonawca związany jest ofertą przez 30 dni od dnia upływu terminu składania ofert tj. do dnia 17.02.2022 r. „

wprowadza się zapis:

” **TERMIN ZWIĄZANIA OFERTĄ**

Wykonawca związany jest ofertą do dnia 19.02.2022 r. „

4. W miejsce zapisu w SWZ Rozdział XII pkt3, 4,5

” 3. W sytuacji, o której mowa w pkt 2 zamawiający zamieści na platformazakupowa.pl. informację o zmianie terminu otwarcia ofert.
4. Zamawiający najpóźniej przed otwarciem ofert, udostępni na platformazakupowa.pl. informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na platformazakupowa.pl. informacje o których mowa w art. 222 ustawy. „

wprowadza się zapis:

” 3. W sytuacji, o której mowa w pkt 2 zamawiający zamieści na https://platformazakupowa.pl/pn/labowa informację o zmianie terminu otwarcia ofert.
4. Zamawiający najpóźniej przed otwarciem ofert, udostępni na https://platformazakupowa.pl/pn/labowa informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

5. Zamawiający, niezwłocznie po otwarciu ofert, udostępni na https://platformazakupowa.pl/pn/labowa informacje o których mowa w art. 222 ustawy. „

5. **W miejsce zapisu w SWZ Rozdział XV pkt 1**
” 1. Zamawiający wymaga wniesienia wadium w wysokości:

1) Część 1 – 6000,00 zł
2) Część 2 – 4900,00 zł
3) Część 3 – 2000,00 zł „

wprowadza się zapis:
” 1. Zamawiający wymaga wniesienia wadium w wysokości:

4) Część 1 – 6000,00 zł
5) Część 2 – 490,00 zł
6) Część 3 – 200,00 zł „

Na podst. art. 284 ust. 3 ustawy z dnia 11.09.2019r. Pr zamówień publicznych (Dz. U. 2019 poz.2019 z późn. zm.) Zamawiający przedłużenia terminu składania i otwarcia ofert w przedmiotowym postępowaniu, wyznaczając nowy termin na dzień:
21.01.2022 r. godzina 10.00 - termin składania ofert
21.01.2022 r. godzina 10.30 - termin otwarcia ofert
Ogłoszenie o zmianie ogłoszenia zostało przesłane do BZP w dn. 14.01.2022 r. i po opublikowaniu zamieszczone na stronie prowadzonego postępowania.

Ponadto, w związku ze zmianą terminu składania i otwarcia ofert w przedmiotowym postępowaniu, Zamawiający dokonuje zmiany treści SIWZ w poniższym zakresie:
W miejsce zapisu w SWZ rozdział XII
„
SPOSÓB ORAZ TERMIN SKŁADANIA OFERT
Ofertę wraz z wymaganymi dokumentami należy umieścić na platformie pod adresem: https://platformazakupowa.pl/pn/labowa **do dnia 17.01.2022r. do godz. 12.00**
1. Otwarcie ofert odbędzie się **w dniu 17.01.2022 r., o godz. 12.30 ”**

wprowadza się zapis:
„SPOSÓB ORAZ TERMIN SKŁADANIA OFERT
Ofertę wraz z wymaganymi dokumentami należy umieścić na platformie pod adresem: https://platformazakupowa.pl/pn/labowa **do dnia 21.01.2022r. do godz. 10.00**
1. Otwarcie ofert odbędzie się **w dniu 21.01.2022 r., o godz. 10.30 ”**

Wykonawcy zobowiązani są uwzględnić powyższe zmiany podczas sporządzania i składania ofert oraz wnoszenia wymaganego wadium.

WÓJT GMINY

MARTA SŁABY