**Opis przedmiotu zamówienia**

# Rozdział I

**SPECYFIKACJA TECHNICZNA SIECI TRANSMISJI DANYCH I DOSTĘPU DO INTERNETU DLA URZĘDU MARSZAŁKOWSKIEGO WOJEWÓDZTWA MAZOWIECKIEGO W WARSZAWIE**

**Struktura dokumentu:**

1. Przedmiot zamówienia:

I.1. Sieć IP VPN MPLS.

I.2. Łącza internetowe.

I.3. Punkty dostępowe Wifi.

I.4. Ochrona oraz mitygacja przed atakami typu DDoS.

I.5. System zaawansowanej ochrony dla stacji końcowych i serwerów Zamawiającego.

I.6. Centralny system chronionego, nadzorowanego dostępu do sieci Internet oraz zasobów publikowanych w Internecie przez Zamawiającego.

1. Wymagania szczegółowe związane z przedmiotem zamówienia.

**SZCZEGÓŁOWY OPIS**

1. **PRZEDMIOT ZAMÓWIENIA:**

I.1. Sieć IP VPN MPLS.

I.2. Łącza internetowe.

I.3. Punkty dostępowe Wifi.

I.4. Ochrona oraz mitygacja przed atakami typu DDoS.

I.5. System zaawansowanej ochrony dla stacji końcowych i serwerów Zamawiającego.

I.6. Centralny system chronionego, nadzorowanego dostępu do sieci Internet oraz zasobów publikowanych w Internecie przez Zamawiającego.

**I.1. SIEĆ IP VPN MPLS**

1. Przedmiotem Zamówienia jest usługa Wirtualnej Sieci Prywatnej o topologii Full Mesh, zbudowanej na bazie wydzielonej operatorskiej sieci MPLS Wykonawcy, odseparowanej od sieci Internet i opartej o łącza kablowe (preferowane światłowodowe). Dostarczona przez Wykonawcę sieć WAN ma zapewnić chroniony, nadzorowany dostęp do zasobów Internetowych dla poszczególnych Placówek Zamawiającego (lokalizacji) oraz zapewnić chroniony, nadzorowany dostęp dla użytkowników Internetu do publikowanych przez Zamawiającego zasobów.
2. Ze względu na przyjętą politykę bezpieczeństwa sieci: Zamawiający nie dopuszcza stosowania radiowych łączy dostępowych. Wymóg świadczenia usług przez łącza kablowe z wyłączeniem technologii radiowej uzasadnione jest jego potrzebami wynikającymi z charakteru wykonywanych zadań, w tym statusu informacji przetwarzanych w systemach informatycznych Zamawiającego.
3. Wszystkie placówki zdefiniowane w Tabeli 1 - muszą zostać dołączone do sieci VPN łączami symetrycznymi o gwarantowanych przepływnościach portów, zgodnie z poniższą tabelą:

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Nazwa placówki | Adres placówki | Prędkość portu dostępowego sieci VPN Zamawiającego |
| LOKALIZACJE WARSZAWSKIE | | | |
| 1 | Skoczylasa | 03-469 Warszawa, ul. Skoczylasa 4 | 4000/4000 Mbps |
| 2 | Jagiellońska | 03-719 Warszawa, ul. Jagiellońska 26 | 4000/4000 Mbps |
| 3 | Bankowy | 00-142 Warszawa, Plac Bankowy 3/5 | 1000/1000 Mbps |
| 4 | Brechta 7 | 03-472 Warszawa,  ul. Brechta 7 | 1000/1000 Mbps |
| 5 | Kijowska | 03-743 Warszawa, ul. Kijowska 10/12A | 1000/1000 Mbps |
| 6 | Kłopotowskiego 5 | 03-718 Warszawa, ul. Kłopotowskiego 5 | 1000/1000 Mbps |
| 7 | Kłopotowskiego 22 | 03-717 Warszawa, ul. Kłopotowskiego 22 | 1000/1000 Mbps |
| 8 | Nowy Zjazd | 00-301 Warszawa,  ul. Nowy Zjazd 1 | 1000/1000 Mbps |
| 9 | Solidarności | 03-402 Warszawa, ul. Solidarności 61 | 1000/1000 Mbps |
| 10 | Chrobrego | 02-479 Warszawa, ul. Chrobrego 29 | 300/300 Mbps |
| LOKALIZACJE POZAWARSZAWSKIE | | | |
| 11 | Ciechanów | 06-400 Ciechanów ul. Wodna 1 | 300/300 Mbps |
| 12 | Ostrołęka | 07-410 Ostrołęka ul. Piłsudskiego 38 | 300/300 Mbps |
| 13 | Piaseczno | 05-500 Piaseczno ul. Puławska 38 | 300/300 Mbps |
| 14 | Płock | 09-402 Płock ul. Kolegialna 19 | 300/300 Mbps |
| 15 | Radom | 26-600 Radom ul. Kościuszki 5a | 300/300 Mbps |
| 16 | Siedlce | 08-110 Siedlce ul. Wiszniewskiego 4 | 300/300 Mbps |
| 17 | Wołomin | 05-200 Wołomin ul. Miła 3 | 300/300 Mbps |
| 18 | Żyrardów | 96-300 Żyrardów ul. 1 Maja 17 | 300/300 Mbps |

Tabela 1. Specyfikacja łączy dostępowych VPN

1. Dodatkowo pomiędzy wskazanymi niżej placówkami musi zostać zestawione łącze Ethernet, zakończone interfejsami optycznymi SM:

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Nazwa placówki | Adres placówki | Prędkość portu |
| 1 | Skoczylasa | 03-469 Warszawa, ul. Skoczylasa 4 | 6000/6000 Mbps |
| Jagiellońska | 03-719 Warszawa, ul. Jagiellońska 26 |
| 2 | Skoczylasa | 03-469 Warszawa, ul. Skoczylasa 4 | 2000/2000 Mbps |
| Brechta 7 | 03-472 Warszawa,  ul. Brechta 7 |

**Wymagania dotyczące sieci IP VPN MPLS**

1. Wykonawca zakończy łącza dostępowe we wszystkich lokalizacjach Zamawiającego stosownymi modemami oraz routerami, które będą podlegały zarządzaniu i serwisowaniu przez Wykonawcę. Wykonawca udostępni podgląd pracy routerów w zakresie interfejsów (w trybie tylko do odczytu), m.in.: ustawiona przepustowość, aktualne obciążenie (w czasie rzeczywistym), błędy interfejsu. Wykonawca umożliwi wykonanie na interfejsie routera podstawowych poleceń diagnostycznych poprawności działania sieci: ping, traceroute.
2. Wykonawca zapewni logiczne i fizyczne sieci WAN z łączami internetowymi będącymi przedmiotem zamówienia.
3. Punkt styku sieci lokalnej Zamawiającego i routerów Wykonawcy będzie zgodny odpowiednio ze standardem IEEE 802.3u (styk RJ45) lub IEEE 802.3ae (10GBase-SR).
4. W każdej Placówce musi zapewnić urządzenie sieciowe będące zakończeniem łącza WAN z funkcjonalnością:
   1. DHCP, DHCP Relay,
   2. Filtrowanie pakietów za pomocą list dostępu
   3. NAT statyczny,
   4. routing statyczny
   5. routing dynamiczny
5. Zamawiający wymaga, aby routery dostarczone przez Wykonawcę były przeznaczone do montażu w standardowej szafie typu Rack 19” Zamawiającego.
6. Wykonawca dostarczy narzędzie monitorujące pracę sieci VPN Zamawiającego oparte o przeglądarkę internetową dowolnego dostawcy.
7. Zamawiający wymaga, aby dla każdej Placówki zostały zapewnione mechanizmy kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej. Przez mechanizmy kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej Zamawiający rozumie wykorzystanie reguł firewall, access-list, ustawianie routingu itp.

**I.2. ŁĄCZA INTERNETOWE**

1. Wymagane medium transmisyjne: łącze światłowodowe.
2. Symetryczny dostęp do sieci Internet o parametrach CIR = EIR w placówkach wymienionych w Tabeli 2.

|  |  |  |  |
| --- | --- | --- | --- |
| LP | Nazwa placówki | Adres placówki | Prędkość |
| 1 | Skoczylasa (tzw. dostępowe) | 03-469 Warszawa, ul. Skoczylasa 4 | 4000/4000 Mbps |
| 3 | Jagiellońska (tzw. dostępowe) | 03-719 Warszawa, ul. Jagiellońska 26 | 4000/4000 Mbps |
| 2 | Skoczylasa (tzw. usługowe) | 03-469 Warszawa, ul. Skoczylasa 4 | 1000/1000 Mbps |

Tabela 2. Specyfikacja łączy dostępowych do Internetu

1. Zamawiający oczekuje, że łącza wymienione w pkt. 2 będą odseparowane od siebie fizycznie i logiczne, z niezależną adresacją. Warunek ten zostanie spełniony przez zapewnienie oddzielnego przyłącza budynkowego, oddzielnych światłowodów oraz oddzielnych urządzeń końcowych.
2. Zapewnienie minimum 16 publicznych adresów IP dla każdego z łącz wymienionych w pkt. 2.
3. Zakończenie łączy u Zamawiającego zgodne odpowiednio ze standardem IEEE 802.3u (styk RJ45) lub IEEE 802.3ae (10GBase-SR).
4. Zapewnienie usługi zapasowego serwera DNS (Secondary DNS).
5. Zapewnienie usługi serwera RevDNS.
6. Możliwość wsparcia dla protokołu BGP v4.0 w czasie trwania umowy.
7. Wykonawca zagwarantuje SLA o następujących parametrach:
   1. Godzinową, roczną dostępność łącza i usług na poziomie co najmniej 99,6%.
   2. Usunięcie awarii w przeciągu max. 8 godzin zagwarantowane przez cały okres świadczenia usługi. Usunięcie awarii lub usterki będzie poprzedzone powiadomieniem ze strony Wykonawcy dedykowanej osoby/osób ze strony Zamawiającego o podjętych działaniach naprawczych.
8. Konieczne przerwy techniczne powinny być planowane w czasie pomiędzy godzinami 18:00 a 6:00 oraz wymagają wcześniejszego uzgodnienia z Zamawiającym (pracownikiem Wydziału Informatyki po stronie Zamawiającego).
9. W przypadku zmiany operatora lub medium transmisyjnego przerwa w dostępności łączy i usług nie może przekroczyć 4 godzin. Przełączanie usług powinno się odbyć w czasie pomiędzy godzinami 18.00 a 6.00.

**I.3. PUNKTY DOSTĘPOWE WIFI.**

1. W placówce **Warszawa, ul. Jagiellońska 26**, we wskazanych przez Zamawiającego miejscach, Wykonawca zainstaluje i uruchomi **min. 5 punktów Wifi** (sale konferencyjne: parter oraz III piętro; pomieszczenia VIP na III i IV piętrze).
2. Wszystkie punkty Wifi mają realizować usługę w ramach jednej sieci WLAN.
3. Sieć Wifi oraz wewnętrzna sieć LAN Zamawiającego muszą być odseparowane fizycznie i logicznie.
4. Sieć Wifi musi zapewnić dostęp do Internetu przez niezależne łącze dostępowe w stosunku do łączy zdefiniowanych w **punkcie I.2. Łącza internetowe.** Zamawiający oczekuje separacji fizycznej i logicznej.
5. Sieć Wifi musi zapewniać dostęp do Internetu z prędkością co najmniej **300/300 Mbps**.
6. Dostęp do sieci Wifi musi być zabezpieczony hasłem autoryzującym.
7. Zamawiający wymaga otrzymania dostępu do panelu zarządzania urządzeniami AccessPoint dla wskazanych po stronie Zamawiającego osób, w celu definiowania kluczy dostępu do sieci Wifi oraz monitorowania podłączonych urządzeń, w tym blokowania klientów.
8. Zamawiający oczekuje zapewnienia wymaganej prawnie retencji danych dla sieci Wifi.

**W celu zrealizowania podstawowego założenia zamówienia, tzn. ochrony i nadzoru, Zamawiający oczekuje dostarczenia, wdrożenia oraz utrzymania przez Wykonawcę następujących elementów.**

I.4. Ochrona oraz mitygacją przed atakami typu DDoS.

I.5. System zaawansowanej ochrony dla stacji końcowych i serwerów Zamawiającego.

I.6. Centralny system chronionego, nadzorowanego dostępu do sieci Internet oraz zasobów publikowanych w Internecie przez Zamawiającego.

**I.4. OCHRONA ORAZ MITYGACJA PRZED ATAKAMI TYPU DDOS**

1. W ramach usługi dostępu do Internetu należy zapewnić ochronę przeciw atakom Distributed Denial of Service (DDoS) typu wolumetrycznego.
2. W celu wykrycia ataków system Wykonawcy powinien monitorować sieć Wykonawcy i analizować strumienie danych z wykorzystaniem protokołu przepływu np. Net Flow.
3. System zabezpieczeń ma być umiejscowiony w sieci Wykonawcy i być przez niego w całości zarządzany. Ma on umożliwić ochronę przed atakami DDoS na adresację IPv4 Zamawiającego do 10 Gbps. Adresację IPv4 zapewnia Wykonawca.
4. Po wykryciu ataku ruch zainfekowany ma zostać przekierowany do specjalnego Centrum Przeciwdziałania Atakom DDoS („Scrubbing Center”) znajdującego się w sieci Wykonawcy. Po odfiltrowaniu ruchu niepożądanego, ruch oczyszczony ma zostać skierowany ponownie do Klienta za pomocą np. FlowSpec, tunelu GRE.
5. Ochrona powinna bazować na różnych rodzajach mechanizmów detekcji, w tym na:
   * 1. przekraczaniu progów dla określonych typów pakietów i protokołów,
     2. analizie profilu ruchu Klienta wykrywanie nieoczekiwanych zmian ruchu w odniesieniu do tego profilu,
     3. sygnaturach.
6. Ochrona przeciw atakom Distributed Denial of Service (DDoS) ma obejmować:
7. monitorowanie ruchu w czasie rzeczywistym, w celu identyfikacji typu i natury ataku,
8. powiadamianie Klienta o podejrzeniu wystąpienia ataku,
9. rozpoczęcie usuwania ataku w porozumieniu z Klientem (możliwe jest automatyczne uruchamianie obrony dla alarmów o wysokim poziomie zagrożenia),
10. modyfikację zestawu użytych mechanizmów przeciwdziałania tak, by uzyskać maksymalny poziom filtracji ruchu niepożądanego przy minimalnym wpływie na ruch prawidłowy.
11. Mitygacja (filtrowanie) ataków ma być realizowana w następującym zakresie:
12. filtrowanie ruchu z błędnymi nagłówkami IP/TCP/UDP
13. odrzucanie lub przepuszczanie na bazie zdefiniowanych dla każdego z klientów filtrów operujących na informacjach w nagłówka warstwy 3-ciej i 4-tej modelu OSI.
14. filtrowanie ruchu na określonych portach UDP na podstawie zawartości pola danych w oparciu o wyrażenia regularne.
15. filtrowanie ruchu na określonych portach TCP na podstawie zawartości pola danych w oparciu o wyrażenia regularne.
16. ochrona przed atakami ze „spoofowanymi” (udawanymi) adresami źródłowymi IP poprzez autentykację sesji TCP, zapytań DNS oraz zapytań HTTP.
17. filtrowanie nieprawidłowych zapytań DNS.
18. ograniczenie zapytań DNS do zadanej wartości zapytań/sek.
19. zapewnienie do 5-ciu filtrów opartych o wyrażenia regularne definiujących zakres stosowania autentykacji DNS oraz ograniczania liczby zapytań DNS.
20. filtrowanie nieprawidłowych zapytań HTTP.
21. blokowanie ruchu od stacji końcowych przekraczających progi dla operacji HTTP na sekundę per serwer lub per URL.
22. zapewnienie do 5-ciu filtrów opartych o wyrażenia regularne definiujących zakres stosowania autentykacji HTTP lub ograniczania liczby zapytań HTTP.
23. filtrowanie ruchu w oparciu o wyrażenia regularne dotyczące nagłówków HTTP.
24. ochrona przez atakami typu „slow Lories”, poprzez resetowanie połączeń, które pozostają nieaktywne przez zadany okres czasu.
25. ochrona przez atakami typu „slow Lories”, poprzez resetowanie sesji TCP, której opaktywność jest poniżej zadanej liczby bajtów przesyłanej w zadanym okresie czasu.
26. wykrywanie ruchu kierowanego z serwerów CDN proxy i zastosowanie algorytmów filtrowania na podstawie oryginalnego źródła ruchu.
27. wykrywanie i filtrowanie pakietów z nieprawidłowymi nagłówkami SSL/TLS lub nagłówkami SSL/TLS, które są poza sekwencją.
28. blokowane sesji, jeżeli podczas negocjacji SSL/TLS klient zażąda nadmiernej ilości metod kryptograficznych lub rozszerzeń użytkownika. Próg dla tych wartości ma być konfigurowalny.
29. wykrywanie i rozłączanie sesji, jeżeli negocjacja SSL/TLS nie zakończy się w zadanym czasie.
30. blokowanie ruchu ze stacji, dla których występuje nadmierna liczba nieprawidłowych, nadmiarowych lub niekompletnych sesji SSL.
31. monitorowanie negocjacji SSL dla wszystkich portów, na których mogą być stosowane aplikacje zabezpieczone protokołem TLS: HTTPS, SMTP, IMAP4, POP, LDAP, IRC, NNTP, TELNET, FTP i SIP.
32. ochrona przed atakami pochodzącym od sieci botnetowych (komputerów zainfekowanych w sposób umożliwiające zdalne sterowanie przez hackerów) poprzez filtrowanie na podstawie na bieżąco aktualizowanych sygnatur zawierających listę adresów IP.
33. ochrona przed atakami pochodzącymi z sieci botnetowych poprzez wykrywanie źródeł ataku o wolumenie przekraczającym zadane wartości. Wartości progowe mają być definiowalne zarówno dla całości ruchu jak i do części ruchu zdefiniowanego za pomocą filtru.
34. uruchamianie mitygacji w celu nauczenia się systemu wartości typowych ruchu, które następnie mogą być wykorzystywane do właściwego ustawiania progów dla algorytmów mitygacji.
35. Dodatkowym parametrem systemu ochrony przeciw DDOS jest maksymalny czas, w jakim do Zamawiającego zostanie wysłane powiadomienie o zaistnieniu potencjalnego ataku na monitorowane usługi. Czas ten liczony jest od wystąpienia zdarzenia i wynosi on 15 minut. Sposób powiadomienia ustalony zostanie na etapie realizacji usługi.
36. Wykonawca zapewni poprzez stronę www dostęp do panelu umożliwiającego prezentację statystyk pochodzących z systemu ochrony przed atakami DDoS. Dostęp zostanie udzielony uprawnionym po stronie Zamawiającego osobom (przewiduje się 4 osoby).

**I.5. SYSTEM ZAAWANSOWANEJ OCHRONY DLA STACJI KOŃCOWYCH I SERWERÓW**

Wykonawca dostarczy, wdroży oraz utrzyma zaawansowany systemu ochrony **1700** stacji końcowych użytkowników oraz serwerów zgodnie z poniższymi wymaganiami funkcjonalnymi:

System musi zapewniać ochronę dla co najmniej **1700** chronionych stacji końcowych (Windows) przez okres 3 lat oraz musi przechowywać logi generowane przez agentów przez okres określony przez Zamawiającego (obecnie 120 dni; parametr ten musi być konfigurowalny przez Zamawiającego).

1. System musi składać się z centralnej konsoli zarządzania chronionymi systemami, zarządzania incydentami i raportowania (w skrócie konsoli) oraz oprogramowania uruchomionego na stacjach końcowych, serwerach i urządzeniach mobilnych tzw. agenta

2. Agent musi umożliwiać instalację i uruchomienie na następujących platformach:

a. Microsoft Windows 10, Microsoft Windows 11

b. Microsoft Windows Server 2016, 2019, 2022

4. Agent musi działać równolegle z istniejącymi w organizacji rozwiązaniami zabezpieczeń stacji końcowych (np. AntyVirus, HIPS, itp.) w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwym oprogramowaniem.

5. Agent musi posiadać możliwość instalacji i uruchomienia na stacjach roboczych z nie więcej niż 2GB pamięci RAM

8. Agent musi integrować się z mechanizmem Windows Security Center oraz umożliwiać użytkownikowi manualne przeskanowanie wybranego pliku.

9. Agent musi posiadać opcję komunikacji z systemem za pośrednictwem proxy webowego

10. Wszystkie mechanizmy ochrony system musi realizować metodami, które nie wykorzystują bazy sygnatur. Ochrona bezsygnaturowa jest wymagana w celu zapewnienia ochrony przed nowymi atakami, które nie zostały opisane przy pomocy sygnatur, czyli tzw. atakami dnia zerowego.

11. System musi posiadać możliwość dodawania i usuwania reguł wbudowanego firewalla ochranianego przez agenta systemu z rozróżnieniem reguł obowiązujących w sieci wewnętrznej i poza siecią wewnętrzną.

12. System musi posiadać możliwość zarządzania zasadami szyfrowaniem dysków systemu ochranianego przez agenta.

13. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB systemu ochranianego przez agenta w zakresie:

a. blokowania podłączenia czytników CD-ROM

b. blokowania podłączania zewnętrznych nośników pamięci flash

c. blokowania podłączania urządzeń przenośnych (typu odtwarzacze mp3, aparaty fotograficzne)

d. tworzenia listy wyjątków od reguły blokowania z określeniem trybu dostępu (tylko odczyt, odczyt i zapis) i atrybutów urządzenia obejmujących producenta i nr seryjny

e. dodawania zablokowanych urządzeń tymczasowo do listy wyjątków na określony okres czasu z określeniem trybu dostępu (tylko odczyt, odczyt i zapis)

14. System musi posiadać mechanizmy ochrony przed wykorzystywaniem znanych i nieznanych luk bezpieczeństwa oprogramowania (ochrona anty-exploit).

15. System na potrzeby ochrony anty-exploit nie może stosować technik analizy exploitów wykorzystujących w jakikolwiek sposób zasoby sprzętowe na potrzeby lokalnego środowiska symulacyjnego typu sandbox lub zwirtualizowany kontener.

16. System w przypadku wykrycia techniki ataku ukierunkowanej na podatną aplikację w celu zablokowania ataku musi zatrzymać proces atakowanej aplikacji oraz zebrać zestaw danych dowodowych obejmujących nazwę chronionego systemu, system operacyjny, tożsamość użytkownika, nazwę procesu, dokładną komendę uruchamiającą proces wraz parametrami i znacznik czasowy

17. System w zakresie ochrony anty-exploit musi zapewniać co najmniej:

a. ochronę przed atakami wykorzystującymi technikę Return Oriented Programming

b. ochronę przed atakami wykorzystującymi technikę Structure Exception Handler

c. mitygację ataków z wykorzystaniem techniki Address Space Layout Randomization oraz Date Execution Prevention

d. ochronę przed atakami wykorzystującymi technikę Null Dereference

e. ochronę przed atakami wykorzystującymi kompilatory typu JIT

f. ochronę przed atakami wykorzystującymi funkcje systemowe do omijania mechanizmu Data Execution Prevention i Address Space Layout Randomization

g. ochronę przed podniesieniem uprawnień

h. ochronę przed nadużyciami Asynchronous Procedure Calls

i. ochronę przed enumeracją pamięci procesu

18. System musi obsługiwać sandboxing, czyli możliwość analizy próbki potencjalnie złośliwego oprogramowania w dedykowanym środowisku celem obserwacji jego zachowań i podjęcia decyzji o szkodliwości próbki w zakresie co najmniej:

a. detekcji i usunięcia mechanizmów mających na celu zaciemnienie kodu binarnego próbki (ang. obfuscation / packing)

b. analizy statycznej próbki i wykorzystania metadanych próbki w połączeniu z algorytmami uczenia maszynowego

c. analizy dynamicznej, gdzie próbka jest uruchamiana a jej zachowanie obserwowane w środowisku wirtualnym

d. analizy dynamicznej, gdzie próbka jest uruchamiana a jej zachowanie obserwowane w środowisku fizycznym

e. obsługi następujących systemów operacyjnych w środowisku analizy: Windows 10 64-bit.

19. Usługa sandbox wykorzystywana przez system musi być realizowana przez sandbox lokalny lub przez sandbox chmurowy zlokalizowany na terenie Unii Europejskiej. W przypadku stosowania sandboxa lokalnego należy przewidzieć rozwiązanie pozwalające na analizę co najmniej 500 próbek na godzinę (VM sandboxing)

20. System dla platform Windows musi realizować ochronę przed uruchomieniem złośliwego oprogramowania co najmniej poprzez:

a. sandboxing

b. lokalną statyczną analizę w połączeniu z uczeniem maszynowym

c. ochronę plików współdzielonych bibliotek DLL

d. ochronę przed złośliwymi makrami w dokumentach pakietu Microsoft Office

e. identyfikowanie ataków poprzez śledzenie i grupowanie pozornie niegroźnych pojedynczych zdarzeń w systemie operacyjnym

f. uruchamianie nieznanych plików tylko jeśli są one cyfrowo podpisane przez zaufanych dostawców oprogramowania

g. kontrolę procesów potomnych

h. blokowanie wykonywania plików z określonych lokalizacji takich jak co najmniej: ścieżka, folder sieciowy, zewnętrzny nośnik pamięci

i. periodyczne i zautomatyzowane skanowanie

j. ochronę plików wykonywanych w formacie PE

24. System musi oferować ochronę przed złośliwym oprogramowaniem szyfrującym dyski (tzw. Ransomware)

25. System musi oferować opcję tworzenia wyjątków dla automatycznych werdyktów systemu z wykorzystaniem unikalnego identyfikatora pliku obliczanego funkcją skrótu np. SHA-256

26. System musi posiadać konsolę formie aplikacji webowej dostępną przy pomocy przeglądarki internetowej

27. Dostęp do konsoli musi być realizowany z zapewnieniem poufności, integralności przesyłanych danych oraz uwierzytelnienia serwera

28. Konsola musi obsługiwać dwuskładnikowe uwierzytelnienie administratorów

29. System musi oferować możliwość zabezpieczenia agenta przed odinstalowaniem przy pomocy hasła oraz wymuszenie zdalnego odinstalowania i zdalnej aktualizacji

30. Konsola systemu musi być w całości utrzymywana przez producenta systemu w zakresie dostarczenia mocy obliczeniowej, wysokiej dostępności, przestrzeni na przechowywanie logów/zdarzeń i aktualizacji

31. Wszystkie dane gromadzone przez system muszą być przechowywane na terenie Unii Europejskiej

32. Konsola systemu musi posiadać możliwość budowy dopasowanych kokpitów (inaczej dashboardów) per administrator, w ramach których prezentowane będą co najmniej:

a. liczba aktywnych i nieaktywnych agentów

b. liczba agentów w funkcji platformy tj. Windows

c. liczba agentów w funkcji wersji oprogramowania

d. liczba chronionych systemów w funkcji wersji aktualizacji silników inspekcyjnych

e. top 10 chronionych systemów powiązanych z największą liczbą incydentów

f. liczba incydentów w funkcji istotności incydentu, gdzie istotność incydentu to np. niska, wysoka, krytyczna

g. liczba incydentów w funkcji rodzaju zagrożenia, gdzie rodzaj zagrożenia to co najmniej malware i exploit

33. Konsola systemu musi posiadać funkcję wyszukiwania z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, adres IP, funkcja skrótu, domena

34. Konsola musi obsługiwać przypisywanie użytkownikom konsoli różnego zakresu dostępu bazującego na rolach (tzw. Role Based Access Control) a w tym co najmniej musi umożliwiać przypisanie co najmniej następujących ról:

a. nieograniczony dostęp w trybie zmiany do wszystkich elementów konfiguracji systemu

b. dostęp tylko do elementów konfiguracji powiązanych z instalacją agenta

c. dostęp tylko do obsługi incydentów

35. System musi posiadać funkcje budowania dopasowanych do potrzeb raportów w formacie PDF udostępniając co najmniej następującą bibliotekę elementów:

a. liczba chronionych systemów w funkcji platformy tj. Windows

b. liczba chronionych systemów w funkcji aktywnych i nieaktywnych agentów

c. liczba chronionych systemów w funkcji wersji agenta

d. liczba chronionych systemów w funkcji wersji aktualizacji silników inspekcyjnych

e. liczba incydentów w funkcji statusu incydentu, gdzie status to np. nowy, rozwiązany, przetwarzany

f. liczba incydentów w funkcji istotności incydentu, gdzie istotność incydentu to np. niska, wysoka, krytyczna

g. liczba incydentów w funkcji rodzaju zagrożenia, gdzie rodzaj zagrożenia to co najmniej malware i exploit

h. top 10 chronionych systemów powiązanych z największą liczbą incydentów

36. System musi umożliwiać określenie harmonogramu, zgodnie z którym będą generowane raporty wraz z opcją wskazania adresu email, na który wygenerowany raport ma zostać wysłany

37. System musi umożliwiać integrację z Active Directory

38. System musi umożliwiać przekazywanie logów do zewnętrznych serwerów SYSLOG zapewniając poufność transmisji z wykorzystaniem TLS

39. System musi umożliwiać integrację z platformą komunikacyjną Slack w celu przekazywania powiadomień

40. System musi umożliwiać filtrowanie logów i powiadomień wysyłanych przy pomocy SYSLOG i Slack co najmniej przy pomocy atrybutu istotność zdarzenia

41. System musi umożliwiać wysyłanie powiadomień na wskazane adresy email

42. System musi umożliwiać przygotowywanie pakietów instalacyjnych agenta

43. System musi umożliwiać zdalne pobranie pakietu supportowego wykorzystywanego do diagnostyki agenta

44. System musi umożliwiać nawiązanie połączenia terminalowego z linią poleceń do system chronionego przez agenta, przy czym musi istnieć możliwość wyłączenia tej funkcji w trakcie instalacji agenta bez możliwości jej późniejszej aktywacji z konsoli systemu

45. System musi umożliwiać pobieranie plików z systemu chronionego przez agenta, przy czym musi istnieć możliwość wyłączenia tej funkcji w trakcie instalacji agenta bez możliwości jej późniejszej aktywacji z konsoli systemu

46. System musi umożliwiać grupowanie systemów z zainstalowanym agentem przy pomocy co najmniej typu systemu (serwer, stacja robocza, urządzenie mobilne), systemu operacyjnego, domeny (dotyczy systemów Windows) i członkostwa w grupie Active Directory (dotyczy systemów Windows) i przypisywania do tak zdefiniowanej grupy wybranej konfiguracji agenta

47. System musi posiadać opcję weryfikacji, czy agent posiada łączność z konsolą

48. System musi odkładać logi audytowe śledzące wszystkie zmiany konfiguracyjne i akcje administratorów wykonywane za pośrednictwem konsoli

49. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień agenta i przypisanie ich do grupy chronionych systemów:

a. maksymalna przestrzeń na logi

b. ukrycie ikony w zasobniku systemowym

c. włączenie i wyłączenie dostępu do zdalnej linii poleceń chronionego systemu

d. włączenie i wyłączenie powiadomień o nawiązaniu połączenia do zdalnej linii poleceń chronionego systemu

e. włączenie i wyłączenie powiadomień użytkownika

f. dopasowanie treści powiadomień użytkownika

g. określenie hasła deinstalacji

h. ochrona przed wyłączeniem procesów agenta

i. włączenie i wyłączenie automatycznej aktualizacji agenta

j. włączenie i wyłączenie uploadu w sieci komórkowej

50. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień ochrony przed wykorzystaniem luk bezpieczeństwa w oprogramowaniu (ochrony anty-exploit) i przypisanie ich do grupy chronionych systemów:

a. włączenie i wyłączenie ochrony dla procesów przeglądarek Internetowych

b. włączenie i wyłączenie ochrony dla procesów systemowych

c. włączenie i wyłączenie ochrony przed nadużyciami wywołań systemowych

d. włączenie i wyłączenie ochrony dla procesów użytkownika

51. System musi umożliwiać skonfigurowanie co najmniej następujących ustawień ochrony przed wykonywaniem złośliwego oprogramowania (ochrona anty-malware) i przypisanie ich do grupy chronionych systemów:

a. włączenie i wyłączenie identyfikowania ataków poprzez śledzenie i grupowanie pozornie niegroźnych pojedynczych zdarzeń w systemie operacyjnym

b. włączenie i wyłączenie ochrony przed atakami typu ransomware

c. włączenie i wyłączenie ochrony przez wykrywanie złośliwych procesów potomnych

d. włączenie i wyłączenie wykrywania złośliwych plików wykonywalnych i określenie czy reakcji (tylko raportowanie, blokowanie, kwarantanna)

e. określenie reakcji w przypadku wykrycia nieznanych plików wykonywalnych: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie

f. określenie listy zaufanych producentów oprogramowania

g. określenie listy zaufanych procesów i folderów, z których można wykonywać pliki

h. włączenie i wyłączenie wykrywania złośliwych makr w plikach pakietu Microsoft Office

i. określenie reakcji w przypadku wykrycia nieznanych plików makr: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie

j. określenie harmonogramu periodycznego automatycznego skanowania dysków z możliwością wykluczenia listy folderów

k. włączenie/wyłączenie ochrony przed wykradaniem haseł

l. włączenie/wyłączenie ochrony przed przekierowaniem standardowych strumieni wejścia i wyjścia na gniazdka sieciowe (tzw. network sockets)

m. określenie reakcji w przypadku wykrycia nieznanych plików makr: wyślij do analizy w sandboxie, wykonaj lokalną analizę statyczną, zablokuj, zezwól na uruchomienie

52. System musi posiadać możliwość dostrajanie działania poszczególnych silników inspekcji a w szczególności możliwość tworzenia wyjątków w ich funkcjonowaniu per nazwa procesu

53. System musi umożliwiać blokowanie uruchamiania plików z zewnętrznych nośników danych takich jak przenośna pamięć flash (usb pendrive) i napęd cd-rom

54. System musi umożliwiać zdalne odcięcie chronionego systemu od dostępu sieciowego z możliwością wskazania listy procesów, które zachowają dostęp do sieci

55. Agent musi posiadać opcję pobierania aktualizacji silników inspekcji od innych agentów w tej samej sieci, które już zostały zaktualizowane w celu oszczędzania pasma łącza Internetowego

**I.6. CENTRALNY SYSTEM CHRONIONEGO, NADZOROWANEGO DOSTĘPU DO SIECI INTERNET ORAZ ZASOBÓW PUBLIKOWANYCH W INTERNECIE PRZEZ ZAMAWIAJĄCEGO**

W zakresie tego elementu Zamawiający wymaga dostarczenia platformy sprzętowej, wykonanie wdrożenia oraz utrzymania centralnego dostępu do zasobów zgodnie z poniższą specyfikacją.

1. Zamawiający wymaga dostarczenia dwóch urządzeń bezpieczeństwa NGF (Next-Generation

Firewall) na brzegach sieci Internet Zamawiającego, mogących działać jako klaster wysokiej

dostępności lub jako dwa niezależne urządzenia.

1. Urządzenia bezpieczeństwa NGF muszą być legalne, fabrycznie nowe, nigdy wcześniej nie używane, pochodzące z legalnego kanału dystrybucyjnego, dopuszczone do obrotu, spełniające normy CE. Nie dopuszcza się urządzeń typu refurbished (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
2. Zamawiający wymaga, aby dostarczane urządzenia bezpieczeństwa NGF oraz jego pakiety oprogramowania były sprawdzone w praktyce rynkowej. Oznacza to, iż oprogramowanie systemowe realizujące wszystkie wymagane funkcje, jak też samo urządzenie, musiało być dostępne na rynku co najmniej 6 miesięcy przed terminem składania ofert.
3. Urządzenia bezpieczeństwa NGF i powiązane z nim oprogramowanie systemowe musi być objęte pełnym serwisem producenta (niedopuszczalne jest proponowanie oprogramowanie np. w wersji Beta) w chwili, i co najmniej w okresie 6 miesięcy przed złożeniem ofert. Za datę jego dostępności Zamawiający przyjmuje publikację konkretnej oferowanej wersji oprogramowania (wersji z pełnym wsparciem) na stronie Producenta rozwiązania.
4. Zamawiający wymaga, aby zaoferowane urządzenia bezpieczeństwa NGF były dostępne i serwisowane przez Producenta oraz nie będą przez niego przewidziane do wycofania ze sprzedaży i wsparcia (ogłoszone tzw. dokumenty End-of-Sale lub End-of-Life lub równoważne) – na dzień składania oferty.
5. Wymagane jest dostarczenie wsparcia producenta urządzeń bezpieczeństwa NGF na cały okres umowy (36 miesięcy). Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjny w trybie 24x7.
6. Zamawiający wymaga:
   1. Bezpośredniej terminacji wewnętrznych sieci LAN na urządzeniach NGF,
   2. Spięcia urządzeń NGF łączem Ethernet w celu zapewnienia ciągłości działania dostępu do sieci Internet. Połączenie to może być realizowane z wykorzystaniem łączy określonych **w** **punkcie: I.1. SIEĆ IP VPN MPLS**. W przypadku niedostępności jednego z urządzeń NGF, Zamawiający oczekuje automatycznego przełączenia usługi działania dostępu do sieci Internet na drugie urządzenie.
   3. Spięcia, a następnie uruchomienia routingu dynamicznego BGP pomiędzy urządzeniami NGF a routerami CE,
   4. dla punktów dostępowych: terminacji publicznej adresacji IP na urządzeniach NGF,
   5. dla punktów dostępowych: translacji NAT/PAT realizowana na urządzeniach NGF,
   6. dostępu do Internetu w oparciu o uwierzytelnianie oraz autoryzację na urządzeniach NGF w oparciu o serwer katalogowy AD Zamawiającego.
   7. wdrożenie niezbędnych polityk bezpieczeństwa (reguł) zgodnie z wytycznymi, które zostaną przekazane Wykonawcy na etapie wdrożenia systemu.
7. Dodatkowo Zamawiający wymaga zapewnienia na styku sieci WAN-LAN ochrony usług cyfrowych Zamawiającego udostępnianych do Internetu (www, poczta, dns, ftp itd.) przed zagrożeniami z sieci internetowej. Usługa powinna zawierać m.in. mechanizmy: flood protection, threat prevention. Zamawiający dopuszcza wykorzystanie urządzeń bezpieczeństwa NGF NextGeneration Firewall zlokalizowanych na brzegach sieci Internet w punktach dostępowych.
8. Centralny system bezpieczeństwa, który będzie zarządzany i utrzymywany przez Wykonawcę, ma umożliwić administratorom Zamawiającego:
   1. samodzielne zarządzanie regułami dostępu do i z sieci Internet,
   2. przeglądanie zarejestrowanych zdarzeń sieciowych,
   3. wykonywanie podstawowych czynności diagnostycznych (ping, tracert, kontrola stanu połączeń).
9. Wymagane jest, aby wszystkie czynności administracyjne wykonywane w systemie bezpieczeństwa przez administratorów Zamawiającego, jak również przez administratorów Wykonawcy, były rejestrowane oraz przechowywane przez czas trwania umowy.
10. Zamawiający oczekuje przeprowadzenia dwudniowego szkolenia z obsługi dostarczonego centralnego systemu bezpieczeństwa dla max. 3 osób ze strony Zamawiającego.
11. Zamawiający wymaga dostarczenia schematu umiejscowienia urządzeń bezpieczeństwa.
12. Szczegółowe wymagania w zakresie wymaganych dwóch urządzeń bezpieczeństwa określa poniższa tabela:

|  |  |
| --- | --- |
| **Nr** | **Wymagania minimalne** |
| 1 | Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19”. Całość sprzętu musi być zarządzana przez jednego producenta. |
| 2 | Urządzenie musi być wyposażone w   * Co najmniej 4 porty 10/100/1000 (RJ45), dopuszcza się uzyskanie tych portów poprzez zastosowanie portów 1 Gigabit Ethernet SFP obsadzonych modułami z RJ45, * Co najmniej 4 portów 1G SFP, * Co najmniej 4 porty 10GE SFP+ obsadzone dwoma modułami optycznymi 10GE SFP+ SR i dwoma modułami optycznymi 10GE SFP+ LR, * Co najmniej 4 porty 40/100 Gigabit Ethernet QSFP28 lub alternatywnie co najmniej 4 porty 40 Gigabit Ethernet QSFP+ i co najmniej 4 porty 100 Gigabit Ethernet QSFP28 * 1 port 1G (RJ45) lub 10G (RJ45) wyłącznie do celów zarządzania, dopuszcza się uzyskanie tego portu poprzez zastosowanie portów SFP / SFP+ obsadzonych modułami z RJ45 * dwa redundantne zasilacze AC 230V Hot-Swap z kompletami kabli, |
| 3 | Urządzenie musi posiadać port (10G lub szybsze) dla celów połączenia urządzeń w klaster (high availability). Porty te muszą być traktowane jako dodatkowe względem wymaganych przez Zamawiającego. Nie dopuszcza się wykorzystania do celu klastrowania portów opisanych w podstawowych wymaganiach. |
| 4 | Urządzenie musi być wyposażone w dysk HDD lub SSD do przechowywania logów i raportów o pojemności nie mniejszej niż 400GB |
| 5 | Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:   * Minimum 45 Gbps dla Firewall/kontroli aplikacji, * Minimum 23 Gbps dla Firewall/IPS/kontroli aplikacji/antymalware, * Minimum 250 tys. nowych połączeń na sekundę, * Minimum 3 mln. równoległych sesji, * 10 wirtualnych routerów posiadających odrębne tabele routingu.   Jako scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych.  Jako scenariusz Firewall/IPS/kontroli aplikacji/antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, antymalware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antymalware, ochrony DNS. |
| 6 | Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy   1. routera (tzn. w warstwie 3 modelu OSI), 2. przełącznika (tzn. w warstwie 2 modelu OSI), 3. w trybie pasywnego nasłuchu (sniffer). |
| 7 | Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu. |
| 8 | Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk. |
| 9 | Urządzenie musi umożliwiać zestawianie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji siteto-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. |
| 10 | Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe:   * Minimum 20 Gbps dla IPSEC VPN * Minimum 10 tys. tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN.   Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (co najmniej dla Windows) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 1700 jednoczesnych użytkowników |
| 11 | Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej   * oznaczania pakietów znacznikami DiffServ, * utworzenia co najmniej 8 klas ruchu sieciowego, * kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. |
| 12 | Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. |
| 13 | Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP. |
| 14 | Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu. |
| 15 | Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active. |
| 16 | Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 5 000 reguł polityki bezpieczeństwa oraz obsługę minimum 50 stref bezpieczeństwa. |
| 18 | Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów, na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Urządzenie musi wykrywać co najmniej 4000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. |
| 19 | Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie. |
| 20 | Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. |
| 21 | Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku, gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji. |
| 22 | Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download”. |
| 23 | Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. |
| 24 | Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu  wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH |
| 25 | Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o:   1. Microsoft Active Directory, 2. usługi katalogowe LDAP, 3. serwery Terminal Services, 4. logi z syslog. |
| 26 | Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. |
| 27 | Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji.  System IPS musi działać w warstwie 7 modelu OSI.  Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia.  Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa)  Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.  Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.  Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia. |
| 28 | Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem.    Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) w celu ochrony przed zagrożeniami typu zero-day.  Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.  Zamawiający musi posiadać dostęp do raportów z sandboxa dotyczących plików wysyłanych przez urządzenia, jak również posiadać możliwość manualnego wysłania pliku (np. poprzez upload przez stronę www) do sandboxa.  Zamawiający wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia. Jeżeli producent rozwiązania dodatkowo licencjonuje liczbę plików przesyłanych automatycznie (przez urządzenie) do chmurowego sandboxa wówczas należy przyjąć wartość 5 000 plików dziennie |
| 30 | Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza. aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.  Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia |
| 31 | Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).  Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia |
| 32 | Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet. |
| 33 | Urządzenie musi posiadać funkcję blokowania ruchu sieciowego w oparciu o IP Geolocation. |
| 34 | Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering.  Baza web filtering musi być regularnie aktualizowana w sposób automatyczny. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa).  Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania.  Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia |
| 35 | Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). |
| 36 | System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu:   1. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu 2. Operator, który ma możliwość tylko odczytu konfiguracji.   Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą   1. bazy lokalnej, 2. serwera LDAP, 3. RADIUS lub TACACS+ 4. SAML 2,0   Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania np. baza lokalna, LDAP i RADIUS |
| 37 | Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.  Realizacja tego wymagania musi opierać się o samo urządzenie – nie dopuszcza się realizacji koncepcji kandydackiej z wykorzystaniem centralnej konsoli zarządzania. Funkcja ta musi być dostępna również w przypadku utraty komunikacji z centralną konsolą zarządzania.  Funkcja ta musi być realizowana co najmniej przez graficzny interfejs zarządzania firewallem (GUI). |
| 38 | Urządzenie musi zapewniać interfejs API (JSON lub REST lub XML lub inny) będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI) |
| 39 | Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. |
| 40 | Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG. |
| 41 | Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie. |
| 42 | Urządzenie musi posiadać funkcjonalność sieciowego Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji. Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb. Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Moduł AV nie może wprowadzać zmniejszenia wydajności urządzenia. |
| 43 | Urządzenie musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur aplikacyjnych (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa. Funkcja ta musi być wbudowana w firewall i nie może wymagać korzystania z rozwiązań trzecich. |
| 44 | Wszystkie wymienione powyżej funkcje muszą być dostępne i realizowane przez urządzenie jednocześnie. Nie jest dopuszczalne, aby realizacja jakiejkolwiek funkcjonalności powodowała konieczność przełączenia urządzenia w inny tryb pracy ograniczający lub uniemożliwiający skorzystanie z innej wymaganej funkcji. Podobnie uruchomienie jakiekolwiek opisanej funkcji nie może spowodować wyłączenia lub ograniczenie działania innej funkcji wymaganej przez Zamawiającego.  Jednocześnie Zamawiający zastrzega sobie prawo do wezwania Wykonawcy do złożenia wyjaśnień oraz prezentacji działania zaoferowanego urządzenia w przypadku powzięcia wątpliwości w tym zakresie. |

**II. WYMAGANIA SZCZEGÓŁOWE ZWIĄZANE Z PRZEDMIOTEM ZAMÓWIENIA**

1. Wykonawca musi posiadać lub dysponować siecią szkieletową.
2. Wykonawca zapewni mechanizm blokujący dostęp do stron Internetowych wymienionych na „Liście ostrzeżeń przed niebezpiecznymi stronami”, publikowanej przez CERT Polska pod adresem: <https://cert.pl/posts/2020/03/ostrzezenia_phishing/>. Rozwiązanie musi wykorzystywać zawsze aktualną „Listę ostrzeżeń przed niebezpiecznymi stronami”. Warunek będzie spełniony, jeśli Wykonawca cyklicznie, przynajmniej 1 raz dziennie, będzie dokonywał implementacji najnowszej opublikowanej przez CERT Polska listy ostrzeżeń.
3. Wykonawca zapewni w każdym czasie okresu realizacji przedmiotu zamówienia możliwość priorytetyzacji ruchu pakietów IP Zamawiającego na całym odcinku sieci (również w sieci Wykonawcy).
4. Wykonawca zdefiniuje w sieci VPN Zamawiającego 1 klasę usługową (Class of service, CoS) dedykowane celom transmisji danych.
5. Zmawiający zastrzega sobie w każdym czasie trwania realizacji przedmiotu zamówienia zmianę ilości klas usługowych (CoS) bez dodatkowych kosztów.
6. Rozszerzenie klas ruchu przez Zamawiającego nie przekroczy 5 klas, w tym dedykowane klasy dla transmisji głosu i obrazu.
7. Procentowy podział pasma łącza dostępowego na klasy ruchu zostanie zdefiniowany przez Zamawiającego.
8. Odwzorowanie ruchu pakietów IP Zamawiającego na CoS sieci VPN musi opierać się o:
   1. znacznik DSCP
   2. znacznik IEEE 802.1p
   3. adresy IP/porty źródłowe/docelowe
9. Wykonawca zagwarantuje całodobowe, telefoniczne wsparcie techniczne przez cały okres świadczenia usługi.
10. Wykonawca zagwarantuje SLA o następujących parametrach:
    1. Godzinową, roczną dostępność placówki na poziomie co najmniej 99,6%
    2. Usunięcie awarii w przeciągu max. 8 godzin zagwarantowane przez cały okres świadczenia usługi. Usunięcie awarii lub usterki będzie poprzedzone powiadomieniem ze strony Wykonawcy dedykowanej osoby/osób ze strony Zamawiającego o podjętych działaniach naprawczych.
    3. W przypadku odwzorowania ruchu pakietów IP Zamawiającego na CoS sieci VPN Wykonawcy, Wykonawca będzie w stanie zagwarantować dla min. dwóch klas ruchu danych średnią (w cyklu dobowym) wartość parametru RTD na dobowym poziomie nie przekraczającym 75 ms. Dodatkowo Zamawiający oczekuje, iż przynajmniej jedna z klas ruchu danych Wykonawcy zagwarantuje średnią dobową wartość parametru LPR na poziomie nie przekraczającym 0,2%.
11. Na żądanie Zamawiającego, Wykonawca będzie zobowiązany do co najmniej jednej w skali miesiąca, bezpłatnej zmiany konfiguracji routerów we wskazanych placówkach. Zmiany konfiguracji routerów mogą dotyczyć m.in. rozszerzenia/zawężenia maski dla obsługiwanych podsieci Zamawiającego, zmiany wynikające z kształtowania i ochrony ruchu sieciowego na poziomie warstwy trzeciej (przez wykorzystanie reguł firewall, access-list, ustawianie routingu) itp.
12. Wszystkie urządzenia dostarczone w ramach realizacji przedmiotu zamówienia i będące w zarządzaniu przez Wykonawcę muszą podlegać cyklicznym aktualizacjom firmware oraz oprogramowania systemowego, nie rzadziej niż 1 raz w roku oraz dodatkowo i niezwłocznie w każdym przypadku opublikowania podatności w zakresie cyberzagrożeń dla tych urządzeń (o ile aktualizacje zostały udostępnione przez producentów urządzeń i oprogramowania). Za wykonanie aktualizacji odpowiada Wykonawca.

# Rozdział II

**Opis przedmiotu zamówienia na świadczenie usług telekomunikacyjnych głosowych w technologii VoIP dla potrzeb Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie.**

1. Przedmiotem zamówienia jest kompleksowe świadczenie usług telekomunikacyjnych głosowych   
   w technologii VoIP dla potrzeb Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie.
2. Czas trwania umowy – 36 miesięcy, rozpoczęcie świadczenia usług od dnia 1 stycznia 2024 roku do dnia 31 grudnia 2026 roku.
3. Zamawiający informuje, że umowa zawarta z obecnym operatorem telekomunikacyjnym wygasa   
   z dniem 31 grudnia 2023 roku.
4. Uruchomienie usług telekomunikacyjnych głosowych w technologii VoIP od 1 stycznia 2024 roku musi się odbyć w sposób pozwalający na nieprzerwaną realizację połączeń telefonicznych przez Zamawiającego. W okresie obowiązywania umowy Wykonawca zobowiązuje się zapewnić stały dostęp do usług telefonicznych dla połączeń wychodzących i przychodzących.
5. Zgodnie z ustawą z dnia 16 lipca 2004 roku *prawo telekomunikacyjne,* świadczona przez Wykonawcę usługa telekomunikacyjna głosowa w technologii VoIP musi mieć charakter powszechny.
6. Wykonawca usług telekomunikacyjnych głosowych w technologii VoIP musi posiadać międzyoperatorskie punkty styku w minimum 10 miastach na terenie Polski.
7. Zamawiający informuje, że użytkuje następujące rodzaje aparatów telefonicznych obsługujących technologię VoIP:
8. Platan model - IP T200G – ilość 1262 szt.,
9. Platan model - IP T216CG – ilość 114 szt.,
10. Platan model - IP T216CGW – ilość 10 szt.,
11. Platan model - IP T202G – ilość 110 szt.,
12. Yealink model SIP-T23G – ilość 64 szt.,
13. Yealink model SIP-T29G – ilość 10 szt.,
14. Yealink model IP W52H – ilość 1 szt.
15. Aparaty telefoniczne, o których mowa w pkt 7 są w posiadaniu Zamawiającego i będą wykorzystywane   
    w trakcie trwania umowy do nawiązywania połączeń za pomocą platformy VoIP. Zamawiający zastrzega możliwość zwiększenia liczby aparatów w trakcie trwania umowy w zależności od zmian ilościowych pracowników zatrudnionych u Zamawiającego.
16. Wykonawca w ramach realizacji usług telekomunikacyjnych głosowych w technologii VoIP zobowiązuje się do programowania aparatów telefonicznych, o których mowa w pkt 7 z uwzględnieniem zapisu   
    w pkt 8 dla poszczególnych użytkowników Zamawiającego w szczególności polegającym na:
17. dodawaniu nowych aparatów telefonicznych do platformy VoIP i ich konfiguracja,
18. przypisywaniu numerów telefonicznych będących w posiadaniu Zamawiającego do poszczególnych aparatów telefonicznych,
19. przypisywaniu użytkowników Zamawiającego do poszczególnych numerów telefonicznych (wyświetlanie osoby dzwoniącej na wyświetlaczu aparatu telefonicznego),
20. konfigurowaniu tzw. grup sekretarsko – dyrektorskich (odpowiednie ustawnie i programowanie   
    w aparatach telefonicznych i platformie VoiP funkcji do obsługi sekretariatów funkcjonujących   
    u Zamawiającego),
21. uruchamianiu dodatkowych funkcji platformy VoIP – między innymi: konfiguracja BLF (monitorowanie stanu innych linii telefonicznych), nagrywanie rozmów dla poszczególnych numerów, fax-u, kolejkowania rozmów, poczty głosowej.
22. Wykonawca zobowiązuje się wykonania czynność określonych w pkt 9, w terminie do 2 dni roboczych od chwili zgłoszenia telefonicznie lub na adres e-mail Wykonawcy.
23. Zamawiający wymaga redundancji geograficznej środowiska systemu telekomunikacyjnego, z którego będzie dostarczona przez Wykonawcę usługa telekomunikacyjna głosowa w technologii VoIP.
24. W ramach świadczenia usług telekomunikacyjnych głosowych w technolog VoIP Wykonawca zobowiązuje się do zapewnienia Zamawiającemu dostępu do platformy VoIP (centrali telefonicznej VoIP) w celu realizacji usług, o których mowa w pkt. 1. Wykonawca zobowiązuje się do utrzymywania przez cały okres umowy sprawnego działania platformy VoIP (wsparcie producenta platformy VoIP), zapewniając możliwość korzystania przez Zamawiającego z jej funkcji.
25. Udostępniona przez Wykonawcę platforma VoIP musi mieć możliwość obsługiwania **min. 4 tysięcy numerów** jednocześnie oraz posiadać możliwość uruchamiania dodatkowych funkcjonalności   
    w zależności od potrzeb Zamawiającego, w szczególności:
26. nagrywanie połączeń,
27. poczta głosowa,
28. mostek konferencyjny,
29. IVR - Interaktywna Odpowiedź Głosowa,
30. BLF - monitorowanie stanu innych linii telefonicznych,
31. CLIP – prezentacja numeru wywołującego,
32. CLIR – blokada numeru telefonu osoby dzwoniącej,
33. przekierowywanie połączeń.
34. Zamawiający wymaga, aby platforma VoIP udostępniona przez Wykonawcę nie była realizowana   
    w oparciu o oprogramowanie Open Source.
35. Wykonawca zobowiązuje się do uruchomienia platformy VoIP za pośrednictwem wydzielonej sieci   
    w pełni odseparowanej od publicznego Internetu.
36. Zamawiający wymaga utworzenia osobnego VLAN-u w sieci LAN Zamawiającego na potrzeby usług telekomunikacyjnych głosowych w technologii VoIP, przy czym Zamawiający informuje, że każda lokalizacja Zamawiającego posiada swoją podsieć połączoną za pomocą MPLS.
37. W ramach realizacji usług telekomunikacyjnych głosowych w technologii VoIP Wykonawca zobowiązuje się dostarczyć do lokalizacji Zamawiającego numerację wskazaną w Tabeli 1, gwarantując przeniesienie numeracji obecnie posiadanej przez Zamawiającego i jej uruchomienie w swojej sieci w pierwszym dniu   
    po zakończeniu okresu obowiązywania umowy u dotychczasowego operatora telekomunikacyjnego.
38. W ramach dostarczonej przez Wykonawcę numeracji, o której mowa w pkt 17 Wykonawca zobowiązuje się do:
39. zachowania obecnej numeracji telefonicznej Zamawiającego, o której mowa w Tabeli nr 1,
40. zarezerwowania w ogólnokrajowym planie numeracyjnym do wyłącznej dyspozycji Zamawiającego zakresu numeracji wymienionej w Tabeli nr 1,
41. realizacji obsługi skróconej numeracji dla wszystkich numerów telefonicznych Zamawiającego niezależnie od lokalizacji numeru,
42. realizowania bezpłatnych połączeń w ramach numeracji Zamawiającego określonej w Tabeli nr 1,
43. sekundowego rozliczania dla połączeń lokalnych, strefowych, międzystrefowych, komórkowych   
    i międzynarodowych bez opłaty za rozpoczęcie połączenia. Pozostałe połączenia, które nie zostały określone w opisie przedmiotu zamówienia, będą rozliczane według cennika Wykonawcy   
    (w szczególności połączenia na numery specjalne),
44. naliczania za nawiązywane połączenia stałej opłaty zgodniej z ofertą Wykonawcy niezależnie   
    od godziny i dnia tygodnia.
45. Wykonawca na prośbę Zamawiającego zobowiązuje się do sporządzania i dostarczania na adres poczty elektronicznej: [administracyjny@mazovia.pl](mailto:administracyjny@mazovia.pl), za każdy okres rozliczeniowy szczegółowego wykazu zrealizowanych połączeń, w formie elektronicznej: dokument MS EXCEL oraz zbiorczego wykazu połączeń zawierającego informację o kierunku, ilości połączeń, czasie trwania i koszcie oraz wykaz zawierający datę, czas trwania i numer połączeń przychodzących. Wykaz połączeń Wykonawca zobowiązuje się dostarczyć w terminie do 7 dni kalendarzowych od chwili zgłoszenia przez Zamawiającego.
46. Wykonawca w ramach świadczonych usług telekomunikacyjnych głosowych w technolog VoIP zobowiązany jest do zapewnienia i udostępnienia w okresie trwania umowy platformy VoIP umożliwiające korzystanie przez Zamawiającego między innymi z następujących rozwiązań telekomunikacyjnych:
47. obsługa min. 2000 numerów Zamawiającego,
48. kolejkowanie rozmów dla min. 10 wybranych numerów,
49. nagrywanie dla min. 15 numerów,
50. poczta głosowa dla min. 10 numerów,
51. fax to mail dla min. 55 numerów,
52. możliwość zaprogramowania BLF (monitorowanie stanu innych linii telefonicznych) dla min 250 numerów Zamawiającego,
53. możliwość zaprogramowania grup sekretarsko-dyrektorskich dla min. 55 numerów,
54. Extension Dialing: funkcja wyboru użytkownika Platformy VOiP poprzez wybranie numeru skróconego (wewnętrznego),
55. Auto Callback: oddzwonienie w przypadku zajętości użytkownika, do którego realizowaliśmy połączenie po czasie, w którym dany użytkownik jest znów wolny,
56. Pick up: przejmowanie połączeń skierowanych,
57. Pick up : przejmowanie połączeń w grupie,
58. Call Forwarding Always: bezwarunkowe przekierowanie wywołania,
59. Call Forwarding Busy: przekierowanie wywołania kiedy zajęty,
60. Call Forwarding No Answer: przekierowanie wywołania gdy nie odbiera, po czasie,
61. Call Forwarding Remote Access: przekierowanie wywołania na numer zewnętrzny,
62. Call Hold: zawieszenie połączenia,
63. Call Return: połączenie zwrotne,
64. Call Transfer with Three-Way Consultation: przeniesienie rozmowy do drugiego użytkownika   
    z możliwością konsultacji,
65. Call Transfer with Third-Party Consultation: przeniesienie rozmowy do drugiego użytkownika   
    z możliwością zestawienia rozmowy trójstronnej,
66. Call Waiting: obsługa połączenia oczekującego,
67. Calling Line ID Blocking Per Call: zakaz prezentacji numeru w czasie jednego połączenia,
68. Calling Name Delivery: prezentacja nazwy użytkownika Platformy VOiP,
69. Calling Line ID Delivery: prezentacja nazwy użytkownika wewnętrznego,
70. Cancel Call Waiting Per Call: usunięcie wybranego wywołania z kolejki,
71. Consultation Hold: konsultacja, zawieszenie,
72. Do Not Disturb: nie przeszkadzać,
73. Last Number Redial: powtórne wybranie numeru telefonicznego,
74. Speed Dial : możliwość powtórnego wybrania jednego z min 10 ostatnio wybieranych numerów,
75. transmisja Faksowa z protokołem T.38,
76. wybieranie w trybie DTMF (sygnalizacja tonowa),
77. informacja o połączeniach przychodzących min. 10 ostatnich numerów.
78. Oferowana platforma VoIP musi być wyposażona w centralny system zarządzania telefonami VoIP posiadanymi przez Zamawiającego. W ramach zaoferowanego systemu zarządzania musi być możliwość automatycznego pobierania poniżej wymienionych parametrów przez telefony VoIP ustawionych   
    w systemie zarządzania:
79. Nazwa użytkownika (login),
80. Hasło uwierzytelniające,
81. Adres serwera rejestracyjnego,
82. Port rejestracyjny SIP,
83. Kodeki,
84. Sposób transmisji DTMF,
85. BLF (Busy Line Field),
86. Włączenie/wyłączenie LDAP,
87. Filtrowanie nazw LDAP,
88. Filtrowanie numerów LDAP,
89. Adres serwera LDAP,
90. Nazwa bazy LDAP,
91. Nazwa użytkownika LDAP,
92. Hasło LDAP,
93. Maksymalna liczba wyników LDAP,
94. Atrybuty nazwy LDAP,
95. Atrybuty numeru LDAP,
96. Nazwa wyświetlana LDAP,
97. Wersja protokołu LDAP,
98. Sortowanie wyników LDAP,
99. Przeszukiwanie LDAP dla połączeń przychodzących,
100. Przeszukiwanie LDAP dla połączeń wychodzących.
101. Wykonawca zobowiązuje się bezpłatnie przeszkolić i nadać uprawnienia wyznaczonym pracownikom   
     Zamawiającego do konfiguracji platformy VoIP na poziomie instalatora do administrowania usługami   
     i numerami wewnętrznymi systemu.
102. Wykonawca udostępni uprawnienia w terminie do 7 dni roboczych od daty uruchomienia usług tj.   
     od 1 stycznia 2024 roku uprawnionym przez Zamawiającego pracownikom panel webowy do centralnego zarządzania konfiguracją aparatów telefonicznych. Wykonawca zapewni 1 dniowe szkolenie w zakresie obsługi panelu webowego. Szkolenie zostanie przeprowadzone w siedzibie Zamawiającego lub on-line. Termin szkolenia zostanie wspólnie uzgodniony przez Strony.
103. Wykonawca zapewni wsparcie techniczne w zakresie obsługi oraz konfiguracji aparatów telefonicznych, w szczególności: aktualizacji firmware, implementacji zabezpieczeń, integracji ze środowiskiem Microsoft (m.in. Active Directory, Certification Authority, Network Access Protection).
104. Wykonawca zobowiązany jest realizować cykliczne aktualizacje firmware aparatów, o których mowa   
     w pkt 7 z uwzględnieniem zapisu w pkt 8 oraz oprogramowania systemowego, nie rzadziej niż 1 raz   
     w roku oraz dodatkowo i niezwłocznie w każdym przypadku opublikowania podatności w zakresie cyberzagrożeń dla tych urządzeń (o ile aktualizacje zostały udostępnione przez producentów urządzeń   
     i oprogramowania).
105. Wykonawca zobowiązany jest bieżąco informować o wszelkich zmianach w zakresie usług telekomunikacyjnych z wyprzedzeniem pozwalającym na podjęcie ewentualnych działań ze strony Zamawiającego.
106. Wykonawca gwarantuje przeniesienie numeracji obecnie posiadanej przez Zamawiającego   
     i jej uruchomienie w swojej sieci w pierwszym dniu po zakończeniu okresu obowiązywania umowy   
     u dotychczasowego operatora.
107. Wykonawcy nie przysługuje prawo do roszczeń w przypadku nie wykorzystania przewidywanych wartości poszczególnych rodzajów usług i dostaw, a w przypadku przekroczenia ich wartości cena będzie liczona według stawek określonych w ofercie Wykonawcy.
108. Zamawiający informuje, że czas połączeń wychodzących telefonicznych za okres 01.01.2023 roku   
     do 31.05.2023 roku (hh:mm:ss) wynosił:
109. Połączenia lokalne (w tym połączenia z pomiędzy numeracją Zamawiającego) 6854:07:50,
110. Połączenia międzystrefowe 353:48:29,
111. Połączenia międzynarodowe stacjonarne UE 04:43:21,
112. Połączenia międzynarodowe stacjonarne 00:55:22,
113. Połączenia międzynarodowe komórkowe UE 03:45:30,
114. Połączenia międzynarodowe komórkowe 02:58:26,
115. Połączenia do sieci komórkowych w Polsce 3245:48:30,
116. Połączenia pozostałe (19x, Biuro Numerów, nr bezpłatne, itp.) 32:13:04.
117. Podany czas trwania połączeń ma charakter szacunkowy ustalony na podstawie dotychczasowych ilości za 5 miesięcy. Rzeczywisty czas trwania połączeń może być inny i nie może mieć to wpływu na wzrost kosztu połączeń / cen jednostkowych usług.
118. Wykonawcy nie przysługuje prawo do roszczeń w przypadku nie wykorzystania przewidywanych wartości poszczególnych rodzajów usług i dostaw, a w przypadku przekroczenia ich wartości cena będzie liczona według stawek określonych w ofercie Wykonawcy.
119. Wykonawca zobowiązany jest do udzielenia informacji w ciągu 14 dni od daty złożenia przez Zamawiającego zapytania na adres e-mail Wykonawcy wskazany w umowie w zakresie możliwości technicznych uruchomienia dodatkowych usług związanych z realizacją umowy w tym określonych   
     w opisie przedmiotu zamówienia. Informacja powinna być wysłana na adres e-mail Zamawiającego wskazany w umowie oraz powinna zawierać szacunkowe koszty związane z uruchomieniem dodatkowych/nowych usług oraz czas w jakim mogą być uruchomione.
120. Wykonawca w ramach świadczenia usług telekomunikacyjnych głosowych w technologii VoiP gwarantuje następujące parametry SLA dla przedmiotowej usługi:

|  |  |  |
| --- | --- | --- |
| L.p. | Parametr | Wartość |
|  | Gwarantowany czas przywrócenia dostępu do usług w przypadku całkowitego braku dostępności | 3h |
|  | Gwarantowany czas naprawy awarii łącza/usługi telefonicznej | 6h |
|  | Dostępność usług VoiP (centrala VoIP) | 98% w ciągu obowiązywania umowy |
|  | Dostępność serwisu dla centrali VoIP i realizowanych rzez nią usług telefonicznych | 24/7/365 |
|  | Czas reakcji na zgłoszenie | 1h |
|  | Miesięczne okno serwisowe (poza godzinami pracy Zamawiającego tj. od 18.00 do 6.00) | 2h raz w miesiącu |

1. Wykonawca umożliwi Zamawiającemu dostęp w terminie do 7 dni roboczych od daty uruchomienia usług tj. od 1 stycznia 2024 roku do portalu Wykonawcy, z którego Zamawiający będzie miał możliwość wykonania/pobrania bilingów i zestawień dla wszystkich numerów telefonicznych Zamawiającego.   
   W udostępnionym systemie Zamawiający powinien mieć możliwość wglądu w następujące dane:
2. datę i godzinę rozpoczęcia rozmowy w formacie DD-MM-YYYY HH:MM:SS (data i godzina mogą występować w osobnych polach);
3. numer abonenta A – wykonującego połączenie (wszystkie cyfry bez przerw i dodatkowych znaków);
4. numer abonenta B – docelowego (wszystkie cyfry bez przerw i dodatkowych znaków);
5. czas połączenia w sekundach [s] lub w formacje HH:MM:SS;
6. kwotę brutto – opłata za rozmowę wyrażona w złotych polskich podana z dokładnością jaką Wykonawca używa do rozliczeń (nie mniej niż 0,01 zł);
7. cenę jednostkową;
8. strefę;
9. rekordy taryfikacyjne uzupełnione o dodatkowe, opcjonalne pola.
10. W przypadku braku możliwości udostępnienia portali www, Wykonawca zobowiązuje się do dostarczenia w formie elektronicznej na płycie CD/DVD lub na e-mail wykazu połączeń za dany okres rozliczeniowy dla poszczególnych numerów Zamawiającego, wymienionych w załączniku nr 1 do niniejszej umowy. Wykaz powinien być przekazany na wskazany przez Zamawiającego adres e-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ w terminie nie dłuższym niż 7 dni roboczych od dnia zakończenia miesiąca rozliczeniowego. Zamawiający wymaga aby szczegółowy wykaz połączeń w formie elektronicznej na płycie CD/DVD lub na e-mail był dostarczony w formie xls/xlsx (EXCEL).
11. Wykonawca zobowiązuje się do realizacji w ramach wynagrodzenia określonego w umowie usługi polegającej na ograniczaniu i włączaniu połączeń na numery o podwyższonej płatności typu 0-70 \_\_\_  
    0-30 i innych numerach o podwyższonej płatności na dowolnym numerze należącym do Zamawiającego.
12. Wykonawca w ramach wynagrodzenia, określonego w umowie zapewni, przeniesienie do będącej   
    w dyspozycji Wykonawcy sieci, dotychczasowych numerów wykorzystywanych przez Zamawiającego, zgodnie z art. 71 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2022 r. poz. 1648 z późn. zm.) oraz Rozporządzeniem Ministra Cyfryzacji z dnia 11 grudnia 2018 roku w sprawie warunków korzystania z uprawnień w publicznych sieciach telefonicznych(Dz.U. z 2018 r. poz. 2324).
13. W przypadku zmiany operatora telekomunikacyjnego przez Wykonawcę w trakcie trwania umowy z winy Wykonawcy koszty prac montażowych związanych z przeniesieniem posiadanych numerów i ewentualnym przeprogramowaniem oraz uruchomieniem usługi dla Zamawiającego pokrywa wyłoniony w postępowaniu Wykonawca
14. O wszelkich planowanych pracach serwisowych mający wpływ na prawidłowe funkcjonowanie usług telekomunikacyjnych głosowych w technologii VoIP Wykonawca zobowiązuje się poinformować Zamawiającego na adres e-mail wskazany w umowie z minimum 48-godzinnych wyprzedzeniem.

Tabela nr 1 - Wykaz aktualnej numeracji wykorzystywanej przez Zamawiającego tj. Urząd Marszałkowski Województwa Mazowieckiego w Warszawie.

| **L.p.** | **Lokalizacje** | **Zakres numeracji Zamawiającego** |
| --- | --- | --- |
| 1 | UMWM w Warszawie:  ul. Jagiellońska 26,  ul. W. Skoczylasa 4  ul. B. Brechta 3  ul. B. Brechta 7  ul. Okrzei 35,  ul. Kłopotowskiego 5  ul. Kłopotowskiego 22  ul. Kijowska 10/12a  ul. Pl. Bankowy 3/5  Al. Solidarności 61  ul. Chrobrego 29  ul. Nowy Zjazd 1  UMWM Delegatura  w Płocku ul. Kolegialna 19  UMWM Delegatura  w Radomiu ul. Kościuszki 5A  UMWM Delegatura  w Ciechanowie ul. Wodna 1  UMWM Delegatura  w Ostrołęce ul. Piłsudskiego 38 UMWM Delegatura  w Siedlcach ul.  Wiszniewskiego 4  UMWM Delegatura w Piasecznie ul. Puławska 38  UMWM Delegatura  w Wołominie ul. Miła 3  UMWM Delegatura  w Żyrardowie ul. 1 Maja 17 | 22 5979 000 do 22 5979 999  22 3141 650 do 22 3141 699  22 3563 800 do 22 3563 899  22 4379 450 do 22 4379 499  22 3141 650 do 22 3141 699  22 5907 600 do 22 5907 899  22 4324 500 do 22 4324 599  22 4324 650 do 22 4324 699  22 5117 400 do 22 5117 499  22 51714 60 do 22 51714 69  22 54390 70 do 22 54390 79  22 620 27 07  22 620 29 44  22 620 13 74  22 632-66-04  22 632-66-07  22 632-66-08  22 863-34-29  22 827 72 38  22 828 84 59  22 827 70 46  22 827 72 54  22 828 84 53  22 828 84 55  22 828 84 56  22 870 27 18  22 870 27 63  24 26732 80 do 24 26732 99  48 36829 60 do 48 36829 79  23 6730 700 do 23 6730 799  29 74441 80 do 29 74441 99  25 63114 40 do 25 63115 59  22 27936 90 do 22 27936 99  22 27936 80 do 22 27936 89  46 81929 70 do46 81929 79 |

**Cześć III: Opis przedmiotu zamówienia w zakresie wsparcia technicznego (w tym „help desk”).**

1. Wykonawca zobowiązany jest do:
2. dostawy wszelkich urządzeń niezbędnych do uruchomienia i świadczenia usług objętych umową oraz zapewni dla nich serwis techniczny w przypadku pojawienia się usterki lub awarii na własny koszt;
3. montażu i konfiguracji przedmiotowych urządzeń w miejscach udostępnionych przez Zamawiającego, po uprzednim uzgodnieniu z Zamawiającym terminu;
4. uruchomienia i przetestowania poprawności działania urządzeń i usług;
5. świadczenia usług na warunkach określonych w specyfikacji oraz Umowie;
6. zdemontowania urządzeń udostępnionych Zamawiającemu na czas trwania umowy po jej wygaśnięciu lub rozwiązaniu.
7. W przypadku niemożliwości usunięcia usterki lub awarii urządzeń/urządzenia, o którym mowa w ust. pkt 1 w ciągu 12 godzin, Wykonawca zobowiązuje się do dostarczenia równoważnego urządzenia/urządzeń sprawnych technicznie w celu prawidłowego świadczenia usług będących przedmiotem umowy.
8. Wykonawca ponosi odpowiedzialność za wady i szkody powstałe w czasie transportu urządzeń do miejsca przeznaczenia oraz za uszkodzenia mienia Zamawiającego z winy Wykonawcy.
9. W zakresie świadczenia usług telekomunikacyjnych głosowych w technologii VoIP zobowiązuje się do zapewnienia prawidłowego działania platformy VoIP oraz innych urządzeń niezbędnych do realizacji przedmiotowej usługi. Przez nieprawidłowe działanie platformy VoIP rozumiane jest w szczególności: występowanie podczas jej eksploatacji awarii, błędów i wad polegających w szczególności na tym, że:
10. platforma VoIP nie funkcjonuje prawidłowo,
11. platforma VoIP nie stanowi kompletnego rozwiązania zgodnie z założeniami opisanymi w opisie przedmiotu zamówienia.
12. Przez awarię rozumie się: nieprawidłowe działanie platformy VoIP powodujące całkowity brak możliwości korzystania lub takie ograniczenie możliwości korzystania, że przestaje on spełniać swoje podstawowe funkcje, uniemożliwiające uzyskanie połączenia na zewnątrz lub na numery wewnętrzne, które dotyka ponad 10 % zasobów. Awarią jest również niemożliwość uruchomienia platformy utrata danych lub ich spójności, niedostępność krytycznych funkcji platformy (uniemożliwiającej korzystanie z usługi).
13. Przez błąd rozumie się: problem polegający na niedostępności wybranych funkcjonalności Platformy VoIP istotnych dla Zamawiającego.
14. Przez wadę rozumie się: inne niż błąd i awaria działanie platformy VoIP niezgodne z wymaganiami funkcjonalnymi i poza funkcjonalnymi, przy prawidłowo działającej infrastrukturze informatycznej Zamawiającego.
15. Zestawienie i uruchomienie usług mogą być dokonywane etapami.
16. Wykonawca zobowiązuje się do świadczenia usługi wsparcia technicznego typu „Help Desk”, polegającego na:
17. przyjmowaniu zgłoszeń o awariach, braku dostępności Usługi i nieprawidłowościach w świadczeniu Usług – telefonicznie, faksem, lub na adres poczty e-mail, dostępne przez całą dobę, każdego dnia, przez cały okres obowiązywania umowy. W przypadku zgłoszeń telefonicznych, Wykonawca zobowiązany jest przy przyjmowaniu zgłoszenia podać przedstawicielowi Zamawiającego numer rejestracyjny zgłoszenia nadany przez serwis Wykonawcy oraz informować o stanie realizacji sprawy wg. numeru rejestracyjnego nadanego podczas zgłoszenia;
18. stałym aktywnym monitorowaniu usług, w tym samodzielnym otwieraniu zgłoszeń problemowych oraz powiadamianiu Zamawiającego o wykrytych problemach – telefonicznie, lub przez pocztę e-mail;
19. udzielaniu porad technicznych związanych ze świadczonymi usługami;
20. rozwiązywaniu problemów zgłoszonych przez użytkowników ze strony Zamawiającego;
21. Usunięcie awarii każdorazowo w pełni przywraca utraconą funkcjonalność.
22. W celu umożliwienia Zamawiającemu dokonywania zgłoszeń, Wykonawca udostępnia dla Zamawiającego czynny całodobowo nr telefonu \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ oraz adres poczty elektronicznej \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ . O każdej zmianie wymienionego wyżej numeru telefonu, i adresu poczty elektronicznej Wykonawca powiadomi Zamawiającego drogą mailową na adres e-mail \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Zmiana ta nie wymaga sporządzania aneksu do umowy.
23. Czas przyjęcia zgłoszenia o awarii lub wykonania usługi wynosi nie dłużej niż 1 godzina, przyjęcie zgłoszenia potwierdzone e-mailem lub telefonicznie na adres\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ tel \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
24. Czas przywrócenia dostępności Usług nie może być dłuższy niż określony w warunkach SLA – szczegółowo określonych w części I i II opisu przedmiotu zamówienia.
25. W razie braku reakcji, nieskutecznej reakcji i braku wsparcia technicznego ze strony Wykonawcy -   
    w terminach określonych w opisie przedmiotu zamówienia, po trzykrotnym zgłoszeniu uszkodzenia bądź problemu przez Zamawiającego, Zamawiający zastrzega sobie prawo do usunięcia uszkodzenia lub rozwiązania problemu przez inny podmiot, na koszt i odpowiedzialność Wykonawcy, co może jednak nastąpić nie wcześniej niż przed upływem 12 godzin od chwili pierwszego zgłoszenia danego uszkodzenia bądź problemu.
26. Zamawiający dopuszcza dwie przerwy techniczne w roku, w preferowanych przez Zamawiającego godzinach 18.00 – 6.00 dnia następnego w celu dokonywania niezbędnych konserwacji urządzeń.

O niniejszych przerwach planowanych Zamawiający będzie informowany z minimum 48-godzinnych wyprzedzeniem na adres email określony w umowie.

1. Zamawiający dopuszcza następujące przerwy podczas przenoszenia usług telekomunikacyjnych - przy zmianie łączności w terminie uruchomienia usługi związanej ze zmianą operatora nie dłużej niż 4 godziny w godzinach od 18.00 do 6.00.