Narodowe Centrum Badań i Rozwoju

ZAPYTANIE O SZACUNKOWĄ WARTOŚĆ ZAMÓWIENIA NA ZAKUP LICENCJI DOSTĘPOWEJ DO OPROGRAMOWANIA KLASY EMAIL SECURITY GATEWAY W MODELU SaaS, NA POTRZEBY NARODOWEGO CENTRUM BADAŃ I ROZWOJU

Narodowe Centrum Badań i Rozwoju (NCBR), z siedzibą w Warszawie (00-695) przy ul. Nowogrodzkiej 47a (NIP: 701-007-37-77, REGON: 141032404) (zwane dalej: „Zamawiającym") planuje wszczęcie postępowania o udzielenie zamówienia publicznego, którego przedmiotem będzie zakup licencji dostępowej do oprogramowania klasy Email Security Gateway w modelu SaaS, na potrzeby Narodowego Centrum Badań i Rozwoju. W związku z powyższym, w celu oszacowania wartości zamówienia Zamawiający zwraca się z prośbą o udzielenie informacji na temat ceny netto oraz brutto całkowitego kosztu realizacji usługi.

I. Przedmiot zamówienia:

Zakup licencji dostępowej do oprogramowania klasy Email Security Gateway w modelu SaaS, na potrzeby Narodowego Centrum Badań i Rozwoju.

II. Kod CPV:

48000000-8: Pakiety oprogramowania i systemy informatyczne
48730000-4: Pakiet oprogramowania zabezpieczającego

III. Opis przedmiotu zamówienia:

1. Przedmiot zamówienia obejmuje:

Zakup licencji dostępowej dla 1001 skrzynek, zgodnej z nw. wymogami technicznymi:

Pozycja	Wymagania funkcjonalne, które rozwiązanie musi posiadać:
Globalne	
Ochrona antyspam i antyphishing	
AS.001	Rozwiązanie musi posiadać moduł antyspamowy i antyphishingowy
AS.002	Rozwiązanie musi posiadać globalną bazę reputacji nadawców dostarczoną przez producenta oferowanego rozwiązania.
AS.003	Rozwiązanie musi posiadać globalną baze sum kontrolnych obiektów spamowych dostarczoną przez producenta oferowanego rozwiązania.
AS.004	Rozwiązanie musi posiadać bazę reputacji nadawców lokalnych (na podstawie IPv4, IPv6 i identyfikacji punktów końcowych)
AS.005	Możliwość kontrolowania i monitorowania ilości przychodzących wiadomości i/lub połączeń z pojedynczego adresu IP i definiowania akceptowalnych poziomów połączeń per adres IP zdalnego hosta. (Sender rate control per connection)
AS.006	Szczegółowa kontrola nagłówków wiadomości przychodzących
AS.007	Walidacja nadawcy (mail from:) poprzez mechanizmy sprawdzające takie jak: SPF, DKIM oraz DMARC

AS.008	Walidacja poprawności adresu email nadawcy na kopercie (adres kopertowy) z nazwą uwierzytelnionego użytkownika (Authentication difference check dla mail from:)
AS.009	Weryfikacja adresu zwrotnego (bounce) za pomocą tagowania.
AS.010	Rozwiązanie musi posiadać aktualną bazę adresów URL i e-mail powiązanych ze spamem, złośliwym oprogramowaniem i atakami typu phishing dostarczoną przez producenta oferowanego rozwiązania.
AS.011	Obsługa w czasie rzeczywistym czarnych list adresów URL wysyłających spam tworzonych przez innych producentów (SURBL/RBL)
AS.012	Obsługa w czasie rzeczywistym blocklist DNSBL.
AS.013	Mechanizm greylistingu dla adresów IPv4, IPv6 i kont poczty e-mail oraz możliwość tworzenia polityk i reguł greylistingowych.
AS.014	Kompleksowe filtrowanie adresów URL z możliwością tworzenia swoich własnych kategorii adresów które mają być filtrowane. Baza adresów URL powinna być dostarczona przez producenta oferowanego rozwiązania.
AS.015	Mechanizm analizy behawioralnej analizującej podobieństwa między skanowanym emailem, a znanym spamem znajdującym się w bazie spamu dostarczonej przez producenta oferowanego rozwiązania.
AS.016	Mechanizm analizy podszywania się (impersonalizacja) - ręczne i automatyczne wykrywanie podszywania się pod adres email/osobę.
AS.017	Mozliwośc wykorzystania zdefiniowanych baz słów dozwolonych, zakazanych oraz słowników w ochronie antyspamowej.
AS.018	Mechanizm skanowania plików graficznych (gif, jpg, png) i określania czy dany obraz zawiera spam.
AS.019	Mechanizm wykrywania newsletterów
AS.020	Mechanizm tworzenia i nauki filtrów bayesian.
AS.021	Możliwość ustawiania progów dla dostępnych w module ochrony AS czynności/warunków wg. których zostaną wyzwolone odpowiednie zdefiniowane przez administratora akcje/profile (np. odrzucanie z powiadomieniem nadawcy, odrzucenie bez powiadomienia, wysłanie do kwarantanny i zaakceptowanie.) na wiadomościach przychodzacych i/lub wychodzących
AS.022	Możliwość definiowania i wykorzystywania zewnętrznych baz RBL
Ochrona AV i ochrona zawartości	
AV.001	Rozwiązanie musi posiadać ochronę antywirusową, antymalware oraz mechanizm DLP
AV.002	Ochrona AV musi posiadać globalną bazę sygnatur wirusów i innego złośliwego oprogramowania dostarczoną przez producenta oferowanego rozwiązania.
AV.003	Mechanizm antywirusowy oparty miedzy innymi na sprawdzaniu sygnatur oraz heurystycznym wykrywaniem behawioralnym
AV.004	Mechanizm neutralizacji zawartości w wiadomościach pocztowych, dokumentach MS Office i PDF (usuwanie makr, zawartości aktywne, załączników)
AV.005	Automatyczne deszyfrowanie archiwów, plików PDF i dokumentów biurowych za pomocą wbudowanych i zdefiniowanych przez administratora list haseł oraz funkcji wykrywania słów w treści wiadomości e-mail
AV.006	Neutralizacja zawartość HTML w wiadomościach e-mail poprzez usunięcie hiperłączy/ przepisanie adresów URL
AV.007	Integracja mechanizmów ochrony antywirusowej z rozwiązaniami

	sandboxowymi.
AV.008	Filtrowanie i skanowanie zawartości według rodzaju plików w załącznikach
AV.009	Możliwość wykrywania typów plików i MIME
AV.010	Tworzenie własnych filtrów plików.
AV.011	Kompleksowe zapobieganie utracie danych dzięki identyfikowaniu i wykrywaniu danych wrażliwych lub zdefiniowanych przez administratora (Data Leak Prevention)
AV.012	Ochrona AV powinna wykorzystywać bazę reputacji nadawców lokalnych (na podstawie IPv4, IPv6 i identyfikacji punktów końcowych)
AV.013	Ochrona AV powinna wykorzystywać mechanizm weryfikacji reputacji nadawców dostarczoną przez producenta oferowanego rozwiązania
AV.014	Możliwość skanowania archiwów zagnieżdżonych
AV.015	Filtrowanie wiadomości przychodzących lub wychodzących przy użyciu użyciem słowników
AV.016	Filtrowanie wiadomości według rodzaju plików w załącznikach
AV.017	Filtrowanie słów zakazanych
AV.018	Kompleksowe zapobieganie utracie danych dzięki identyfikowaniu źródła (zasób sieciowy, komputer użytkownika), wykrywaniu danych wrażliwych lub zdefiniowanych przez administratora (Data Leak Prevention)
AV.019	Możliwość ustawiania progów dla dostępnych w module ochrony AV i DLP czynności/warunków wg. których zostaną wyzwolone odpowiednie zdefiniowane przez administratora akcje/profile (np. odrzucanie z powiadomieniem nadawcy, odrzucenie bez powiadomienia, wysłanie do kwarantanny i zaakceptowanie.) na wiadomościach przychodzacych i/lub wychodzących
Szyfrowanie i cyfrowa tożsamość	
SZ.001	Bezagentowa możliwość szyfrowania na podstawie tożsamości w trybie „Push” i „Pull”
SZ.002	Obsługa standardu S/MIME w szyfrowaniu między serwerami pocztowym
SZ.003	Obsługa protokołu SMTP over SSL,
SZ.004	Możliwość zdefiniowania polityk szyfrowania wiadomości na podstawie treści lub odbiorcy
DDoS	
DD.001	Mechanizm ograniczenie liczby połączeń, jednoczesnych połączeń i wiadomości przychodzących i wychodzących
DD.002	Sprawdzanie zapytań revDNS (zapobieganie podszywaniu się pod nadawcę)
DD.003	Ochrona przed fałszowaniem adresów nadawców (adresy kopertowe)
Wymagania dot. SaaS	
SS.001	Wszystkie wymagane środowiska muszą zostać wdrożone, uruchomione i użytkowane w Centrach Danych znajdujących się wyłącznie na terenie państw EOG.
SS.002	Zamawiający wymaga SLA na poziomie nie mniejszym niż 99,999% tj. nie wiecej niż 6 minut przestoju w pracy Systemu rocznie.
SS.003	Komunikacja powinna odbywać się w sposób bezpieczny i szyfrowany. W przypadku integracji z systemami wewnętrznymi Zamawiającego Wykonawca jest odpowiedzialny za zestawienie bezpiecznego i szyfrowanego połączenia z infrastrukturą Centrum. Połączenie to musi być kompatybilne z infrastrukturą

	Zamawiającego, a zakres uzgodniony z Zamawiającym.
SS.004	Wykonawca jest odpowiedzialny za zarządzanie infrastrukturą, nadzór nad ciągłością działania, aktualizacje systemu, monitorowanie ruchu i poziomu wykorzystanych zasobów, rozwiązywania zgłaszanych problemów/incydentów.
SS.005	Wykonawca będzie wykonywał przynajmniej raz dziennie kopie zapasowe danych systemu i udostępniał je Zamawiającemu na życzenie.
SS.006	Wykonawca jest odpowiedzialny za zapewnienie, że wszystkie dane są szyfrowane na źródle (przed opuszczeniem firmowej sieci) oraz podczas ich transferu i przechowywania. Musi się to odbywać bez negatywnego wpływu na współczynnik redukcji danych.
SS.007	Wykonawca jest odpowiedzialny za zapewnienie ochrony przed atakami DDoS, niezbędnych zapór ogniowych i innych środków bezpieczeństwa teleinformatycznego.
SS.008	Wykonawca jest odpowiedzialny za zapewnienie odpowiednio wydajnego środowiska wymaganego do optymalnej pracy Systemu, zgodnie z wymaganiami Zamawiającego.
SS.009	Rozwiązanie musi być zgodne z międzynarodowymi standardami i wytycznymi dotyczącymi bezpieczeństwa, takimi jak ISO 27001, w celu utrzymania działania infrastruktury obliczeniowej i zapewnienia prywatności danych.
SS.010	Wykonawca musi zapewnić ścisłe procedury uwierzytelniania użytkowników i administratorów.
SS.011	Wykonawca musi zapewnić procedury i środki umożliwiające monitorowanie wszystkich operacji przeprowadzanych w systemie informacyjnym oraz raportowanie, zgodnie z obowiązującymi przepisami, w przypadku wystąpienia incydentów dotyczących danych klienta.
SS.012	Wykonawca musi zapewnić, że konfiguracja zasobów współdzielonych uniemożliwia wzajemny dostęp do danych na nich ulokowanych poprzez różne podmioty.
SS.013	Wykonawca musi niezwłocznie powiadomić Zamawiającego o każdym przypadku naruszenia zasad bezpieczeństwa, wtargnięcia lub prośby agencji rządowych o dostęp do danych, aby umożliwić Zamawiającemu zarządzanie tymi wydarzeniami proaktywnie.
SS.014	Wykonawca musi zapewnić, że w przypadku zwolnienia zasobów wszystkie bloki pamięci i wszelkie kopie danych, jeśli takie istnieją, zostaną tak usunięte bądź wyzerowane przez Wykonawcę, aby dane nie mogły zostać odzyskane.
SS.015	Wykonawca nie może przetwarzać ani przechowywać danych Zamawiającego poza EOG.
SS.016	Wykonawca jest zobowiązany do przetwarzania danych osobowych klienta wyłącznie do celów związanych z właściwą realizacją usług i wyłącznie zgodnie z jego instrukcjami.
SS.017	Dane przechowywane na infrastrukturze Wykonawcy pozostają własnością Zamawiającego.
SS.018	Wykonawca musi posiadać system zarządzania uprawnieniami ograniczający dostęp do pomieszczeń oraz danych tylko do osób, które muszą go mieć ze względu na pełnione funkcje i zakres obowiązków.

SS.019	Wykonawca musi określić wspólnie z Zamawiającym zasady przeszukiwania, retencji i usuwania danych dostarczonych przez Zamawiającego.
SS.020	Wykonawca musi raportować wszystkie incydenty bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych przez Zamawiającego w chmurze oraz udzielić Zamawiającemu wszelkiej możliwej pomocy przy zwalczaniu skutków takich incydentów bezpieczeństwa.
SS.021	Rozwiązanie musi mieć zdolność korzystania z zewnętrznego systemu autoryzacji (potencjalnie dostarczonego w przyszłości przez Zamawiającego) wraz z funkcjonalnością SSO na podstawie standardów wymienionych w pozostałych wymaganiach.
SS.022	Rozwiązanie powinno mieć możliwość autoryzowania użytkowników w zewnętrznym repozytorium LDAP i AD. Komunikacja z zewnetrznymi repozytoriami winna odbywać się w sposób bezpieczny.
SS.023	Rozwiązanie musi wspierać połączenie z systemem SSO przynajmniej przy użyciu jednego z następujących standardów: SAML, Oauth, OpenID
SS.024	System musi umożliwiać dodawanie, usuwanie i modyfikację użytkowników i grup
SS.025	Delegowani użytkownicy powinni móc zarządzać całością uprawnień dla grup i użytkowników
SS.026	Delegowani użytkownicy powinni móc tworzyć grupy i nowych użytkowników
SS.027	System musi umożliwiać czasowe blokowanie kont przez administratorów oraz ich odblokowywanie.
SS.028	System musi przechowywać logi pełnej historii zdarzeń takich jak (ale nie ograniczonych do): logowanie i próby logowania, operacje na zasobach, modyfikacje uprawnień użytkowników, dodawanie grup i użytkowników, kasowanie obiektów
SS.029	System rejestruje aktywności Użytkowników (login, adres IP, nazwa komputera, czas).
SS.030	System weryfikuje ważność hasła. Ważność hasła powinna wygaszać po upływie określonej w konfiguracji liczbie dni. System wymusza zmianę hasła. Hasła nie mogą się powtarzać w okresie określonej w konfiguracji liczbie miesięcy.
SS.031	Zamawiający wymaga aby dokumentacja API była publicznie dostępna i nie stanowiła tajemnicy firmy.
SS.032	W przypadku zastosowania gotowego oprogramowania dokumentacja producenta tego oprogramowania musi zostać dołączona do dokumentacji technicznej całego Systemu

2. Rozliczenie umowy:

Rozliczenie umowy nastąpi jednorazowo, po dostarczeniu licencji i potwierdzeniu przez Zamawiającego faktu jej otrzymania;

3. Zamawiający zastrzega sobie możliwość naliczenia kar umownych, w tym co najmniej:

30% w razie niewykonania przedmiotu zamówienia,

10% za każdy przypadek nienależytego wykonania przedmiotu zamówienia,

a także w przypadku przekroczenia terminów wskazanych w umowie.

IV. Termin realizacji zamówienia:

W zależności od wybranej opcji umowa zawarta zostanie na okres 18, 24 lub 36 miesięcy.

Dostawa licencji w terminie do 10 dni kalendarzowych od podpisania umowy.

Zamawiający na etapie szacowania wartości zamówienia zastrzega sobie możliwość negocjacji wskazanych terminów.

V. Miejsce oraz termin przedłożenia informacji o koszcie usług:

Drogą e-mailową na adres karolina.zych@ncbr.gov.pl i slawomir.ponikowski@ncbr.gov.pl do dnia **13 października 2020 r. do godz. 23.59.**

VI. Wycena powinna być złożona na załączonym formularzu wyceny szacunkowej:

FORMULARZ WYCENY SZACUNKOWEJ

PEŁNA NAZWA WYKONAWCY: .....

ADRES Z KODEM POCZTOWYM: .....

TELEFON: …….…….....

ADRES E-MAIL: .....

NUMER NIP:……..…….....

NUMER REGON: .....

Wycena

Nawiązując do zapytania o szacunkowy koszt wykonania zamówienia publicznego, którego przedmiotem będzie zakup licencji dostępowej do oprogramowania klasy Email Security Gateway w modelu SaaS, na potrzeby Narodowego Centrum Badań i Rozwoju, wyceniamy wykonanie przedmiotu zamówienia, w pełnym rzeczowym zakresie ujętym w zapytaniu, za cenę:

Na okres 18 miesięcy dla 1001 skrzynek

netto: …… zł

brutto: ……..… zł

za realizację przedmiotu zamówienia,

Na okres 24 miesięcy dla 1001 skrzynek

netto: …… zł

brutto: ……..… zł

za realizację przedmiotu zamówienia,

Na okres 36 miesięcy dl 1001 skrzynek

netto: …… zł

brutto: ……..… zł

za realizację przedmiotu zamówienia,

Oświadczamy, że:
1. Nie wnosimy żadnych zastrzeżeń do zapytania o szacunkowy koszt.

2. Przyjmujemy do wiadomości, że:
   2.1. złożenie wyceny na zapytanie o szacunkowy koszt, jak też otrzymanie w jego wyniku odpowiedzi nie jest równoznaczne z udzieleniem zamówienia przez Narodowe Centrum Badań i Rozwoju (nie rodzi skutków w postaci zawarcia umowy);
   2.2. powyższe zapytanie szacunkowe nie stanowi oferty w rozumieniu Kodeksu Cywilnego;
   2.3. Zamawiający dopuszcza możliwość doprecyzowania lub skorygowania zapisów i warunków niniejszego zapytania;
   2.4. Zamawiający zastrzega sobie prawo do unieważnienia zapytania szacunkowego bez podania przyczyny.
3. Oświadczam, że wypełniłem/-am obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO*) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu złożenia wyceny w niniejszym postępowaniu**.
   **rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*
   *** W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*
4. Oświadczam, że uzyskałem zgody osób biorących udział w przygotowaniu wyceny, a także wyrażam zgodę na przetwarzanie moich danych osobowych przez Narodowe Centrum Badań i Rozwoju z siedzibą w Warszawa 00-695, Nowogrodzka 47a, i przyjmuję do wiadomości, że moje dane podane w wycenie będą przetwarzane w celu związanym z przygotowaniem postępowania.

…… …….

miejscowość, data podpis, imię i nazwisko

lub podpis na pieczęci imiennej