POLITECHNIKA GDAŃSKA

Dział zamówień publicznych

Gdańsk, data 02.01.2020 r.

dot. postępowania o udzielenie zamówienia prowadzone w trybie przetargu nieograniczonego na dostawę wielostanowiskowej licencji oraz trzyletniej subskrypcji na oprogramowanie antywirusowe wraz z wdrożeniem dla Politechniki Gdańskiej ZP/320/055/D/19

Zamawiający na podstawie art. 38 ust. 2 i ust. 4 ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 z późn. zm.) informuje, iż do Zamawiającego wpłynęło pytanie dotyczące treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ), na które Zamawiający udziela odpowiedzi.

Pytanie 1:
Zamawiający w opisie wymagań w sekcji ochrona stacji roboczych wymaga cytuję "ochrona sieci : możliwość ukrywania portów dla wybranych sieci". Co zamawiający rozumie pod pojęciem ukrywania portów? Czy zamawiający zaakceptuje rozwiązanie oferujące blokowanie komunikacji dla określonych portów TCP/UDP w obu kierunkach?

Odpowiedź:
Zamawiający wyjaśnia, iż przez ukrywanie portów, Zamawiający rozumie otwieranie komunikacji dla wybranych portów TCP/UDP tylko dla aplikacji zdefiniowanych w regułach polityki bezpieczeństwa.
Zamawiający zaakceptuje rozwiązanie oferujące blokowanie komunikacji dla określonych portów TCP/UDP w obu kierunkach jako równoważne.

Pytanie 2:
Zamawiający w opisie wymagań w sekcji ochrona stacji roboczych wymaga cytuję "możliwość przełączania zapory w tryb uczenia". Czy zamawiający zaakceptuje rozwiązanie nie oferujące trybu uczenia dla zapory sieciowej natomiast oferujące ręczne definiowanie reguł dla zapory sieciowej a następnie ich stosowanie oraz dodatkowo oferujące integrację z modułem HIPS, jeśli aplikacja jest na czarnej liście jej komunikacja sieciowa będzie blokowana przez zaporę sieciową?

Odpowiedź:
Zamawiający wyjaśnia, iż uzna taką funkcjonalność jako równoważną z zaporą sieciową oferującą tryb uczenia.

Pytanie 3:
Zamawiający w opisie kryteriów dodatkowych, którymi zamawiający będzie się kierował przy wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego wymienia kryterium Rozszywanie SSL oraz precyzuje że Zamawiający uzna kryterium za spełnione, jeżeli Wykonawca zapewni możliwość rozszywania i inspekcji protokołu SSL w oparciu lub przy pomocy posiadanego przez Zamawiającego urządzenia firmy Checkpoint. Proszę o doprecyzowanie tego kryterium? Czy

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 24 00
faks +48 58 347 29 13
e-mail: dzp@pg.edu.pl
www.pg.edu.pl

zamawiający uzna kryterium za spełnione jeżeli Wykonawca zaoferuje oprogramowanie antywirusowe oferujące skanowanie połączeń szyfrowanych SSL\TLS i nie wykorzystującego do tego urządzeń firm trzecich?

Odpowiedź:
Zamawiający wyjaśnia, iż przez kryterium "Rozszywanie SSL" Zamawiający rozumie integrację pakietu antywirusowego z posiadanym urządzeniem firmy Checkpoint czyli z Sandbox'em, gdzie dokonywana jest emulacja i tym samym wykrywanie zagrożeń związanych z otwarciem lub zapisaniem na dysku załączników lub innych treści przesłanych w tunelu SSL. Zamawiający chce zatem wykorzystać posiadane urządzenie do emulacji w środowisku wirtualnym (sandbox) treści przesyłanych w połączeniu SSL.

Powyższe odpowiedzi stanowią integralną część SIWZ.

Termin składania i otwarcia ofert nie ulega zmianie.

Udzielona odpowiedź będzie wiążąca dla wszystkich Wykonawców, którzy otrzymali SIWZ oraz opublikowane na stronie www.dzp.pg.edu.pl zgodnie z art. 38 ust. 2 i 4 ustawy Pzp.

Kanclerz
Politechniki Gdańskiej
mgr inż. Mariusz Miler

.....
(podpis kierownika zamawiającego
lub osoby upoważnionej)

POLITECHNIKA GDAŃSKA
ul. G. Narutowicza 11/12
80-233 Gdańsk
tel. +48 58 347 24 00
faks +48 58 347 29 13
e-mail: dzp@pg.edu.pl
www.pg.edu.pl