POLITECHNIKA GDAŃSKA

Kanclerz

Gdańsk, 05.10.2016 r.

l.dz. 503 /DZP/2016

dot.: postępowania na dostawę wraz z usługą wdrożenia urządzeń do transmisji danych cyfrowych dla Centrum Usług Informatycznych Politechniki Gdańskiej – ZP/240/055/D/16.

ZAPYTANIA I WYJAŚNIENIA

Na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164, z późn. zm.), w imieniu Zamawiającego Politechniki Gdańskiej, ul. G. Narutowicza 11/12, 80-233 Gdańsk, informuję, że w postępowaniu wpłynęły od Wykonawców zapytania dotyczące treści Specyfikacji Istotnych Warunków Zamówienia, na które Zamawiający poniżej udziela wyjaśnień.

Zapytanie 1:
dot. zastosowania odpowiedniej stawki VAT w kontekście opisu przedmiotu zamówienia
W cześć III SIWZ Zmawiający przedstawił elementy przedmiotu zamówienia, którymi są:

1) *„Dostawa systemu bezpieczeństwa sieciowego składającego się z następujących elementów:*
   a) *dwóch urządzeń pełniących funkcję bram bezpieczeństwa sieciowego działających w ramach klastra wysokiej dostępności […] wraz z zestawem odpowiednich licencji zapewniających ciągłość pracy w przypadku awarii jednego z urządzeń,*
   b) *jednego urządzenia pełniącego funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym,*
   c) *systemu zarządzania politykami bezpieczeństwa oraz konfiguracji urządzeń*
   d) *systemu korelacji zdarzeń i raportowania,*

   wraz z subskrypcją na kompleksową usługę w celu utrzymania ciągłości pracy systemu bezpieczeństwa sieciowego, których rodzaje i warunki określone są w Załączniku nr 2 do Umowy;
2) *Usługę wdrożenia systemu bezpieczeństwa sieciowego*
3) *Przeszkolenie personelu Zamawiającego"*

Zgodnie z Załącznikiem 2 do Umowy- *Gwarancja oraz rodzaj i warunki świadczonych* usług *„w przypadku wystąpienia awarii Wykonawca zobowiązuje się do jej usunięcia w miejscu użytkowania sprzętu (on-site) z czasem reakcji do następnego dnia roboczego, tzw. Next Business Day licząc od momentu ich zgłoszenia przez Zamawiającego […]".*
Zgodnie z zapisem §3 ust. 7 wzoru umowy Zmawiający wystąpi do MNiSW o wydanie poświadczenia celem zastosowania 0% stawki VAT do urządzeń do transmisji danych cyfrowych.
W związku z przytoczonymi wyżej informacjami Wykonawca pragnie zauważyć, iż w myśl Załącznika nr 8 do ustawy o podatku od towarów i usług gdzie przedstawiono zamknięty katalog urządzeń, tylko urządzenia do transmisji danych cyfrowych składające się na przedmiot zamówienia, mogą zostać dostarczone z 0% VAT.
Dla pozostałych elementów przedmiotu zamówienia takich jak: licencje do systemów, rozwiązania aplikacyjne, oprogramowanie inne niż wbudowane w urządzenie, subskrypcje, elementy urządzeń (np. wkładki, kable), usługi wdrożenia, szkolenia czy serwisu musi zostać zastosowana stawka VAT 23%.
W związku z powyższym, Wykonawca zwraca się do Zamawiającego o jednoznaczne

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

potwierdzenie, iż wystąpi o możliwość zastosowania VAT 0% wyłączenie dla urządzeń do transmisji danych cyfrowych - dopuszczonych ustawą.
Wykonawca wnosi również o jednoznacznie potwierdzenie, iż w formularzu „Oferta" należy przyjąć w pkt. 1 cenę brutto z uwzględnieniem stawki VAT w wysokości 23% dla wszystkich komponentów przedmiotu zamówienia (w tym urządzeń cyfrowych). Jest to o tyle istotne, iż na etapie składania ofert Zamawiający nie może zakładać a priori, iż zakupi urządzenia z preferencyjną stawką 0%VAT gdyż to zależy od ziszczenia się okoliczności, które wystąpią w późniejszym etapie procesu zakupowego.
Co więcej, jednoznaczne określenie, iż wszyscy wykonawcy uczestniczący w postępowaniu mają zastosować do wszystkich elementów przedmiotu zamówienia tę samą, podstawową stawkę podatku (23%) pozwala Zamawiającemu uzyskać oferty w pełni porównywalne.

Wyjaśnienie:
Zamawiający wystąpi o możliwość zastosowania VAT 0% dla urządzeń do transmisji danych cyfrowych wraz z kompleksową usługą zapewniającą utrzymanie ciągłości pracy systemu bezpieczeństwa sieciowego, na którą składa się rozszerzona gwarancja, w ramach której Wykonawca będzie zobowiązany do usuwania awarii, wymiany uszkodzonych elementów, uaktualniania oprogramowania oraz udzielania pomocy technicznej.
Usługa wdrożenia systemu bezpieczeństwa sieciowego oraz przeszkolenie personelu Zamawiającego zostaną wydzielone w Formularzu rzeczowo-cenowym (załączniku nr 3 do SIWZ), jako odrębne pozycje.
Dla wszystkich pozycji w Formularzu rzeczowo-cenowym, Wykonawca winien zastosować stawkę zgodną z obowiązującymi przepisami.
Wykonawca, któremu zostanie udzielone zamówienie, zastosuje stawkę podatku VAT 0% na fakturze, po otrzymaniu stosownego zaświadczenia. Jeżeli Ministerstwo Nauki i Szkolnictwa Wyższego nie przyśle zaświadczenia w terminie wystawiania faktury, Wykonawca wystawi fakturę z zastosowaniem stawki podatku VAT 23%, a po otrzymaniu ww. zaświadczenia zostanie wystawiona faktura korygującą podatek VAT do stawki 0%.

Zapytanie 2:
dot. § 7 projektu umowy
W § 7 projektu umowy Zamawiający przewidział kary na zasadzie opóźnienia. W myśl art. 476 Kodeksu cywilnego opóźnienie oznacza poniesienie przez Wykonawcę odpowiedzialności zarówno za działanie przez niego zawinione, jak i niezawinione. Wobec tego Wykonawca wnioskuje o wprowadzenie do umowy odpowiedzialności na zasadzie zwłoki. Wówczas Wykonawcy zostaną naliczone kary umowne w przypadku zawinionego przez niego niedotrzymania terminów przewidzianych umową.

Wyjaśnienie:
Zamawiający nie wyraża zgody na zmianę zapisu. Zgodnie z art. 473 § 1 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t.j. Dz. U. z 2016 r. poz.380), Wykonawca może przyjąć na siebie odpowiedzialność za niewykonanie lub za nienależyte wykonanie zobowiązania z powodu oznaczonych okoliczności, za które na mocy ustawy odpowiedzialności nie ponosi. W granicach zakreślonych ramami swobody umów strony mają możność innego niż to przewiduje art. 472 Kodeksu cywilnego uregulowania odpowiedzialności dłużnika.

Zapytanie 3:
dot. okresu rękojmi za wady
Wykonawca prosi o doprecyzowanie czy należy przyjąć standardowy okres rękojmi za wady – t.j. 24 miesiące liczone od protokołu odbioru urządzeń?

Wyjaśnienie:
Tak, ale z zastrzeżeniem przepisu art. 579 § 3 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny.

Zapytanie 4:
dot. pkt II.2.2.2. Szczegółowego Opisu Przedmiotu Zamówienia

Czy Zamawiający dając w pkt. X.4 OPZ możliwość wykorzystania posiadanych przez Zamawiającego licencji do uruchomienia funkcjonalności opisanych w OPZ zgadza się również na wykorzystanie posiadanych przez Zamawiającego ośmiu sztuk wymiennej optyki 10GE SFP+ LR kompatybilnej z oferowanymi urządzeniami?

Wyjaśnienie:
Nie.

Zapytanie 5:
dot. pkt II.2.2.2. Szczegółowego Opisu Przedmiotu Zamówienia
Jeżeli Zamawiający nie zgadza się na wykorzystanie posiadanej przez siebie wymiennej optyki 10GE SFP+ LR, to czy Zamawiający oczekuje dostarczenia zamienników oryginalnych wkładek kompatybilnych z oferowanymi urządzeniami czy też Zamawiający wymaga dostarczenia optyki pochodzącej od producenta tych urządzeń?

Wyjaśnienie:
Zamawiający zgadza się na dostarczenie takich modułów światłowodowych, które nie będą przeszkodą w realizacji zgłoszeń serwisowych u producenta.

Zapytanie 6:
dot. pkt III 2.2) Specyfikacji Istotnych Warunków Zamówienia
Czy Zamawiający obok usługi wdrożenia systemu bezpieczeństwa sieciowego oczekuje:
a) Przygotowania projektu systemu bezpieczeństwa sieciowego?
b) Przygotowania dokumentacji powykonawczej systemu bezpieczeństwa sieciowego?

Wyjaśnienie:
Zamawiający nie oczekuje przygotowania projektu systemu bezpieczeństwa sieciowego. Zamawiający oczekuje natomiast przeniesienia aktualnej konfiguracji systemu bezpieczeństwa na nowo dostarczony system bezpieczeństwa oraz przygotowania dokumentacji powykonawczej.

Zapytanie 7:
W zakresie części II pkt 3.2.5: Czy Zamawiający dopuści urządzanie spełniające w zakresie IPv6 następujące RFC: RFC 6829, RFC 6147, RFC 6146, RFC 6106, RFC 5952, RFC 5881, RFC 5798, RFC 5340, RFC 5308, RFC 5175, RFC 5095, RFC 4941, RFC 4862, RFC 4861, RFC 4443, RFC 4380, RFC 4213, RFC 3956, RFC 3736, RFC 3633, RFC 3587, RFC 3493, RFC 3484, RFC 3315, RFC 3306, RFC 3226, RFC 3056, RFC 3053, RFC 2894, RFC 2893, RFC 2740, RFC 2675, RFC 2545, RFC 2474, RFC 2461, RFC 2460, RFC 2185, RFC 1933, RFC 1883, RFC 1195, RFC 2080, RFC 2080, oraz posiadające certyfikacje IPv6 ReadyPhase 2?

Wyjaśnienie:
Tak, jeśli podane w zapytaniu dokumenty RFC zastępują te, wymagane przez Zamawiającego w części II pkt 3.2.5.

Zapytanie 8:
W zakresie część II pkt. 3.7.6.a: Czy Zamawiający dopuści urządzenie pozwalające na weryfikacje stanu stacji podczas podłączenia, co najmniej w zakresie: zainstalowanego oprogramowanie antywirusowego, zainstalowanych najnowszych poprawek systemu operacyjnego, zainstalowanej wersji firewalla, weryfikacji wpisów w rejestrze, weryfikacji sumy kontrolnej dowolnego pliku, procesu uruchomionego w systemie, weryfikacji wersji systemu operacyjnego, weryfikacji adresu MAC?

Wyjaśnienie: Tak.

Zapytanie 9:
W zakresie części III pkt 1.13 i 1.14 wymaganie brzmi:
„1.13. Moduł dostarczania bezpiecznych plików musi wspierać, co najmniej następujące

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

formaty:
a) Pakiet Microsoft Office: doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xla, xlam, xlm, xls, xlsb, xlsm, xll, xlsx, xlt, xltm, xltx, xlw
b) Pdf, fdf
1.14. Proces bezpiecznego dostarczania plików musi być realizowany, na co najmniej dwa sposoby: a) Konwersja do statycznego pliku pdf b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików".
W części VIII natomiast, posiadanie przez „Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day" funkcjonalności bezpiecznego dostarczania plików wymienione jest, jako wymaganie dodatkowe. Czy można, zatem uznać, że posiadanie przez „Urządzenie pełniące funkcję bez sygnaturowego wykrywania ataków zero-day" takiej funkcjonalności jest tylko wymaganiem dodatkowym? Jeśli Zamawiający potwierdza ww. założenie prosimy o przeniesienie pkt 1.13 i 1.14 z Sekcji III do części VIII w wymaganiach dodatkowych.

Wyjaśnienie:
Tak, posiadanie przez „Urządzenie pełniące funkcję bez sygnaturowego wykrywania ataków zero-day" funkcjonalności opisanej w SIWZ w części III pkt 1.13 i 1.14 jest tylko wymaganiem dodatkowym. Zmiany z treści SIWZ:
W części III pkt 1.13 i 1.14 zostają wykreślone. Część VIII otrzymuje brzmienie:
1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej.
2. Moduł dostarczania bezpiecznych plików musi wspierać co najmniej następujące formaty:
a) Pakiet Microsoft Office: doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xla, xlam, xlm, xls, xlsb, xlsm, xll, xlsx, xlt, xltm, xltx, xlw
b) Pdf, fdf
3. Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików
4. Administrator musi mieć możliwość utworzenia listy adresatów oraz nadawców poczty e-mail, którzy mają być wykluczeni z inspekcji plików.

Zapytanie 10:
W zakresie części III pkt 1: Czy Zamawiający dopuści następujące brzmienie pkt 1.8:
1.8. System do wykrywania ataków zero-day musi umożliwiać następujące reakcje podejmowane w stosunku do pobieranych plików:
a) Pobierany plik nie musi być blokowany, jego skanowanie wykonywane musi być w tle
b) Pobierany plik uznany za podejrzany musi być blokowany, co najmniej do czasu zakończenia inspekcji.

Wyjaśnienie:
W ocenie Zamawiającego zaproponowany zapis jest równoważny z zapisem istniejącym pkt 1.8. Zatem urządzenia spełniającego którykolwiek z zapisów będzie uznane za spełniające SIWZ w niniejszym zakresie.

Zapytanie 11:
W zakresie części III pkt 2.2 i 2.4: Czy Zamawiający dopuści, aby urządzenie do wykrywania ataków zero-day traktować, jako koherentny ekosystem złożony z urządzenia bezpieczeństwa oraz urządzenia do wykrywania ataków zero-day, w którym sumaryczna liczba portów jest stała i wynosi 40 w tym 8 x 10Gb oraz 40 x 1Gb (24 x Base-T oraz 18 x SFP) a przepustowość inline równa jest przepustowości osiąganej w tym zakresie przez urządzenie bezpieczeństwa i wynosi nie mniej niż 5Gbps? W ramach wspomnianego systemu wszystkie wymienione porty mogą być wykorzystywane do przysłania ruchu poddanego analizę zero-day.

Wyjaśnienie:
Zamawiający dopuści urządzenie do wykrywania ataków zero-day o minimalnej liczbie ośmiu

interfejsów 1Gb. Zamawiający rezygnuje z konieczności dostarczenia urządzenia z możliwością rozbudowy do 17 interfejsów za pomocą modułu rozszerzeń.

Zapytanie 12:
W zakresie części IV pkt 5: Czy Zamawiający dopuści, aby zarządzanie politykami bezpieczeństwa oraz CA odbywało się z dwóch niezależnych konsol przy założeniu, że wszystkie komponenty rozwiązania wymienione w Sekcji, w tym CA tworzą jeden spójny ekosystem pochodzącym w całości od jednego producenta?

Wyjaśnienie:
Tak

Zapytanie 13:
W zakresie części VII pkt 1: Czy Zamawiający dopuści urządzenie posiadające bazę witryn WEB wynoszącą nie mniej niż 250 000 000 oraz komplementarne bazy sygnatur aplikacyjnych i IPS zawierające nie mniej niż 10 000 pozycji, z czego co najmniej 5000 sygnatur wyróżniających aplikacje.

Wyjaśnienie:
Nie

Zapytanie 14:
W zakresie części VI czy zamawiający dopuści możliwość rozbudowy urządzenia przez dedykowane, pochodzące do tego samego producenta zewnętrzne moduły sieciowe, w pełni integrujące się z urządzeniem, rozszerzające ilość widzianych przez nie portów, zarządzane z jednej konsoli i pozwalające rozbudowę o do 512 portów 40G lub 768 portów 10G/1G lub wybranej kombinacji portów 1G/10G/40G.

Wyjaśnienie:
Nie

Zapytanie 15:
Wymaganie: „Urządzenia muszą pochodzić od jednego producenta.
Czy zamawiający dopuszcza zastosowanie urządzenia innego producenta w celu realizacji funkcjonalności Clientless VPN w sytuacji gdy oba rozwiązania integrują się na poziomie przekazywania informacji o użytkownikach? Zastosowanie oddzielnego rozwiązania obsługującego dostęp do zasobów sieciowych przez VPN zapewnia bardzo dużą elastyczność konfiguracji systemu bezpieczeństwa oraz zwiększa jego funkcjonalność.

Wyjaśnienie:
Tak, pod warunkiem spełnienia wymagań zawartych w opisie przedmiotu zamówienia w części II pkt. 3.4 oraz pkt. 3.7 oraz wymagania dotyczącego redundancji urządzeń.

Zapytanie 16:
Wymaganie: „Urządzenia muszą pochodzić od jednego producenta."
Czy zamawiający dopuszcza realizację funkcjonalności bezsygnaturowego wykrywania ataków zero-day przez innego producenta niż dostarczone rozwiązania firewall przy zachowaniu funkcjonalności systemu bezpieczeństwa?

Wyjaśnienie:
Zamawiający nie oczekuje dostarczenia samej funkcjonalności bezsygnaturowego wykrywania ataków zero-day, lecz wymaga by była ona realizowana przez fizyczne urządzenie zainstalowane w serwerowni Zamawiającego. W przypadku dostarczenia urządzenia realizującego funkcjonalność bezsygnaturowego wykrywania ataków zero-day od innego producenta niż urządzenia pełniące funkcję bram bezpieczeństwa, Zamawiający uzna, że funkcjonalność systemu bezpieczeństwa została zachowana, jeżeli urządzenie to będzie integrowało się w pełni z systemem zarządzania politykami bezpieczeństwa oraz konfiguracji urządzeń.

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

Zapytanie 17:
Wymaganie: „Każde urządzenie musi być wyposażone przynajmniej w następujące interfejsy :
6 interfejsów 10GE SFP+ z czterema wkładkami typu LR o zasięgu 10km oraz co najmniej dwoma wkładkami typu SR o zasięgu 330m.„
Czy zamawiający dopuszcza rozwiązanie wyposażone w 4 interfejsy 10GE SFP+, 8 interfejsów 1GE SFP oraz 12 interfejsów 1GE RJ45?

Wyjaśnienie:
Nie

Zapytanie 18:
Wymaganie: „Urządzenie powinno charakteryzować się: b) dostępną pamięcią RAM min. 32GB"
Wiele konstrukcji firewall jest wspieranych przez dedykowane układy sprzętowe. Realizują one określone funkcje nie korzystając z globalnych zasobów platformy jak RAM. Podawanie parametrów konstrukcyjnych w przypadku takich rozwiązań nie jest miarodajne ponieważ ilość pamięci nie wpływa na wydajność i funkcje urządzenia. Uwzględniając ten fakt, czy zamawiający dopuszcza urządzenia spełniające wszystkie parametry funkcjonalne oraz wydajnościowe bez względu na ilość pamięci RAM ogólnego przeznaczenia?

Wyjaśnienie:
Zamawiający dopuści zastosowanie urządzenia spełniającego wymogi funkcjonalne oraz wydajnościowe, przy niespełnieniu wymagania na pojemność pamięci RAM jeśli Wykonawca dostarczy oświadczenie producenta urządzenia o zapewnieniu wsparcia oraz aktualizacji oprogramowania przez kolejne 6 lat.

Zapytanie 19:
Wymaganie: „Urządzenie musi realizować inspekcję stanową z wydajnością nie mniejszą niż 30Gbps z możliwością uzyskania do 77Gbps dla pakietów 1518UDP (maksymalna osiągalna wydajność w warunkach testowych zgodnych z RFC 3511, 2544, 2647, 1242). „
W przypadku platform bezpieczeństwa klasy NGF istotna jest wydajność jaką urządzenie osiąga po uruchomianiu funkcji bezpieczeństwa. Przyjmuje się, że inspekcja stanowa (L4) nie zapewnia już wystarczającego poziomu bezpieczeństwa. Czy zamawiający dopuszcza rozwiązania o wydajności 10Gbp w przypadku kontroli Aplikacyjnej (L7) oraz 5Gbps w przypadku kontroli wszystkimi dostępnymi modułami bezpieczeństwa?

Wyjaśnienie:
Zamawiający jako bazę do sprawdzenia wydajności urządzeń przyjął ogólnodostępne procedury testowania opisane w wymienionych RFC. W związku z tym podtrzymujemy brzmienie punktu dotyczącego wydajności.

Zapytanie 20:
Wymaganie: „Urządzenie musi obsługiwać co najmniej 12 800 000 jednoczesnych sesji/połączeń z prędkością zestawiania co najmniej 185 000 połączeń na sekundę.
Podane wymagania znacznie przekraczają realne wartości występujące w sieciach o wielkości Politechniki Gdańskiej. Z doświadczeń oferenta wynika iż w sieciach o rozległości oraz złożoności podobnej do struktury Politechniki Gdańskiej ilość jednoczesnych sesji wynosi ok. 1'000'000 oraz przeciętna ilość nowych sesji na sekundę wynosi ok. 50'000 sesji na sekundę. Czy zamawiający dopuszcza rozwiązanie, które pozwala na utrzymanie 2'000'000 jednoczesnych sesji aplikacyjnych oraz 120'000 nowych sesji na sekundę.

Wyjaśnienie:
Nie. Zamawiający postawił takie wymagania ponieważ przewiduje użytkowanie zamawianego urządzenia przez okres minimum 6-8 lat w ciągu których przewiduje znaczny wzrost ruchu sieciowego.

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

Zapytanie 21:
Wymaganie: „Urządzenie musi obsługiwać protokół SNMP 1/2/3"SNMP v1 jest protokołem niezabezpieczonym, który nie jest zalecany w implementacji. Czy zamawiający dopuszcza urządzenia posiadające wsparcie dla SNMP v2c oraz SNMP v3?

Wyjaśnienie:
Zamawiający nie tylko dopuszcza co wręcz wymaga wsparcie dla protokołu SNMP v2c oraz SNMP v3.

Zapytanie 22:
Wymaganie: „Baza znanych aplikacji musi zawierać nie mniej niż 2 500 pozycji"
Każdy producent inaczej definiuje aplikacje. W wyniku podawania wielu wersji tej samej aplikacji bazy mogą się znacznie różnić ilością rekordów. Czy zamawiający dopuszcza rozwiązanie posiadające zdefiniowane co najmniej 2250 aplikacji oraz mechanizmy umożliwiające tworzenie własnych sygnatur?

Wyjaśnienie:
Tak.

Zapytanie 23:
Wymaganie: „Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików"
Wymagana funkcjonalność jest unikalna dla rozwiązań firmy CheckPoint. Stanowi to ograniczenie konkurencyjności do jednego producenta. Wnosimy o usunięcie powyższych wymagań z SIWZ.

Wyjaśnienie:
W części III pkt 1.13 i 1.14 zostają wykreślone. Część VIII otrzymuje brzmienie:
1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej.
2. Moduł dostarczania bezpiecznych plików musi wspierać co najmniej następujące formaty:
a) Pakiet Microsoft Office: doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xla, xlam, xlm, xls, xlsb, xlsm, xll, xlsx, xlt, xltm, xltx, xlw
b) Pdf, fdf
3. Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików
4. Administrator musi mieć możliwość utworzenia listy adresatów oraz nadawców poczty e-mail, którzy mają być wykluczeni z inspekcji plików.

Zapytanie 24:
Wymaganie: „Urządzenie musi posiadać minimum 9 interfejsów 10/100/1000 BASE-T z możliwością rozbudowy do 17 interfejsów za pomocą modułu rozszerzeń.
Czy zamawiający dopuszcza rozwiązanie, w którym urządzenie do wykrywania ataków zero-day („sandbox") korzysta z interfejsów inline firewall? Urządzenie nie pracuje jako osobne urządzenie inline, ale analizuje ruch przekierowany firewall.

Wyjaśnienie:
Nie, Zamawiający nie dopuszcza rozwiązania które w celu wykrycia ataków zero-day musi wysłać dane poza sieć Zamawiającego.

Zapytanie 25:
Wymaganie: „Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej."
Czy zamawiający dopuszcza dostarczenie funkcjonalności bezsygnaturowego wykrywania ataków zero-day w postaci usługi? Zastosowanie takiego modelu umożliwia zwiększenie limitów ilości analizowanych plików. Zapewnia również wyższy poziom bezpieczeństwa, gdyż środowisko wyniesione jest w stanie uruchomić znacznie więcej maszyn wirtualnych, tym samym dokonać analizy przy użyciu większej ilości wersji i konfiguracji systemów operacyjnych.

Wyjaśnienie:
Nie, Zamawiający nie dopuszcza rozwiązania które w celu wykrycia ataków zero-day musi wysłać dane poza sieć Zamawiającego.

Zapytanie 26:
Dotyczy załącznika nr 1 do Specyfikacji Istotnych Warunków Zamówienia.
Zamawiający wymaga dostarczenia kilku oddzielnych urządzeń pochodzących od jednego producenta realizujących różne funkcje systemu bezpieczeństwa. Nie podaje jednak żadnych wymagań funkcjonalnych uzasadniających konieczność zastosowania rozwiązań pochodzących od jednego producenta. Każdy z wymienionych funkcjonalności tj. brama bezpieczeństwa, urządzenie do bezsygnaturowego wykrywania ataków zero-day, system zarządzania, system korelacji zdarzeń można zrealizować stosując rozwiązania różnych producentów przy zachowaniu określonych dla nich funkcjonalności.
Zastosowany przez Zamawiającego opis przedmiotu zamówienia nie zapewnia zachowania uczciwej konkurencji. Opis przedmiotu zamówienia wskazuje jednocześnie konkretnego producenta firmę Checkpoint i fikcyjnie umożliwia zaoferowanie urządzeń równoważnych.

1) Czy Zamawiający dopuści zaoferowanie systemu bezpieczeństwa zbudowanego w oparciu o rozwiązania różnych producentów zapewniające pełną współpracę i spełnienie wymagań funkcjonalnych?

   Wyjaśnienie:
   Zamawiający dopuszcza zaoferowanie systemu bezpieczeństwa zbudowanego w oparciu o rozwiązania różnych producentów w odniesieniu do:
   a) odrębnego urządzenia realizującego funkcjonalność Clientless VPN pod warunkiem spełnienia wymagań zawartych w opisie przedmiotu zamówienia w części II pkt. 3.4 oraz pkt. 3.7 oraz wymagania dotyczącego redundancji urządzeń.
   b) urządzenia realizującego funkcjonalność bezsygnaturowego wykrywania ataków zero-day pochodzącego od innego producenta niż urządzenia pełniące funkcję bram bezpieczeństwa. Zamawiający uzna, że funkcjonalność systemu bezpieczeństwa została zachowana, jeżeli urządzenie to będzie integrowało się w pełni z systemem zarządzania politykami bezpieczeństwa oraz konfiguracji urządzeń.

   W przypadku zaoferowania urządzeń pochodzących od różnych producentów, na podstawie części VI pkt. 31 SIWZ Wykonawca zostanie poproszony o prezentację pełnej współpracy i spełnienie wymagań funkcjonalnych oferowanego systemu bezpieczeństwa.

2) Czy Zamawiający dopuszcza zastosowanie urządzenia innego producenta w celu realizacji funkcjonalności głębokiej inspekcji pakietów w sytuacji, gdy są one wzajemnie certyfikowane?

   Wyjaśnienie:
   Nie.

3) Czy Zamawiający dopuszcza zastosowanie urządzenia spełniającego wymogi funkcjonalne, przy niespełnieniu parametrów ściśle sprzętowych, jak np. pojemność pamięci RAM, czy pojemność i typ pamięci masowej? Należy zaznaczyć, że ze względu na różną architekturę stosowaną przez producentów parametr posiadanej ilości pamięci RAM w tej klasie urządzeń nie ma znaczenia i wpływu na parametry wydajnościowe i funkcjonalne urządzeń.

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

Wyjaśnienie:
Zamawiający dopuści zastosowanie urządzenia spełniającego wymogi funkcjonalne oraz wydajnościowe, przy niespełnieniu wymagania na pojemność pamięci RAM jeśli Wykonawca dostarczy oświadczenie producenta urządzenia o zapewnieniu wsparcia oraz aktualizacji oprogramowania przez kolejne 6 lat.

4) Czy Zamawiający dopuszcza zastosowanie urządzenia o przepustowości 60 Gbps dla stanowego firewalla, oraz 11 Gbps dla wszystkich włączonych modułów bezpieczeństwa i głębokiej inspekcji pakietu? Są to parametry znacznie przekraczające rzeczywiste potrzeby organizacji o skali uczelni wielkości Politechniki Gdańskiej.

Wyjaśnienie:
Nie. Zamawiający postawił takie wymagania ponieważ przewiduje użytkowanie zamawianego urządzenia przez okres minimum 6-8 lat w ciągu których przewiduje znaczny wzrost ruchu sieciowego.

5) Czy Zamawiający dopuszcza zastosowanie urządzenia utrzymującego 12 700 000 jednoczesnych sesji/połączeń i możliwości zestawiania 240 000 nowych sesji/połączeń na sekundę? Są to parametry znacznie przekraczające rzeczywiste potrzeby organizacji o skali uczelni wielkości Politechniki Gdańskiej.

Wyjaśnienie:
Nie.

6) Czy Zamawiający dopuszcza zastosowanie urządzenia innego producenta w celu realizacji funkcjonalności identyfikacji użytkownika poprzez dedykowanego agenta instalowanego na stacji końcowej?

Wyjaśnienie:
Nie.

7) Czy Zamawiający dopuszcza zastosowanie urządzenia zawierającego bazę 1800 pozycji aplikacyjnych, jednakże obsługiwanych poprzez ponad 2500 sygnatur behawioralnych, opisujących zachowania funkcyjne poszczególnych członów aplikacji? Należy zaznaczyć, że ze względu na różna klasyfikację stosowaną przez producentów przy określaniu aplikacji, bezpośrednie porównanie ilości wpisów w bazie nie jest miarodajne.

Wyjaśnienie:
Nie.

8) Czy Zamawiający dopuszcza zastosowanie urządzenia zawierającego bazę 95 predefiniowanych serwisów/protokołów w sytuacji, gdy możliwe jest własne predefiniowanie kolejnych obiektów?

Wyjaśnienie:
Nie. Zaakceptujemy rozwiązanie, które w momencie dostarczenia będzie zawierało wymaganą liczbę zdefiniowanych serwisów/protokołów, zgodnie z częścią II pkt. 3.1.4. Obiekty mogą być dodefiniowane przez Wykonawcę.

9) Czy Zamawiający dopuszcza zastosowanie urządzenia niewykrywającego wersji językowej systemu, który się łączy i jest filtrowany pod kątem URL przy jednoczesnej możliwości customizacji komunikatów o zablokowanych treściach. Zauważyć należy, że prawdopodobnie zdecydowana większość użytkowników Zamawiającego wyposażona jest w polską wersję systemu operacyjnego.

Wyjaśnienie:
Nie. W środowisku Zamawiającego pracują komputery z wersjami systemów operacyjnych różnych części świata.

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

10) Czy Zamawiający dopuszcza współpracę OEM w przypadku funkcjonalności bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym, z innym podmiotem w którego chmurze ta funkcjonalność będzie realizowana?

Wyjaśnienie:
Nie.

11) Czy Zamawiający dopuszcza zastosowanie urządzenia innego producenta w celu realizacji funkcjonalności clientless VPN w sytuacji gdy oba rozwiązania będą zintegrowane na poziomie informacji o użytkowniku?

Wyjaśnienie:
Odpowiedź na to pytanie została udzielona w odpowiedzi na pytanie 1.

12) Czy Zamawiający dopuszcza zastosowanie urządzenia niewspierającego korelacji zdarzeń z poziomu CheckPoint SmartEvent? Należy zauważyć, że podany system SmartEvent obsługuje tylko urządzenia firmy Checkpoint.

Wyjaśnienie:
Wymaganie współpracy z oprogramowaniem SmartEvent jest wymaganiem dodatkowym.

13) Czy Zamawiający dopuszcza zastosowanie urządzenia niewspierającego raportowania w formacie html a wspierającego raportowanie do csv, pdf.

Wyjaśnienie:
Tak.

14) Czy Zamawiający dopuszcza zastosowanie urządzenia pozwalającego na rozbudowę o dodatkowe interfejsy sieciowe ilościach : 8 portów 1GB RJ45, 8 portów 1GB SFP, 4 porty 10GB SFP+ bez wsparcia dla modułów 40GE QSFP+?

Wyjaśnienie:
Nie.

15) Czy Zamawiający dopuszcza zastosowanie urządzenia w którym sygnaturalna kontrola aplikacji nie jest rozróżniana ze względu na środowisko działania i tym samym widgety WEB 2.0 nie są rozpoznawane?

Wyjaśnienie:
Zamawiający nie zgadza się na zmiany zapisu w części VII pkt 1 opisu przedmiotu zamówienia odnoszącej się do wymogu rozpoznawania widgetów WEB 2.0.

16) Czy Zamawiający dopuszcza zastosowanie urządzenia w którym wersjonowanie konfiguracji i możliwość pracy na minimum pięciu zapisanych konfiguracjach wymaga zewnętrznego zasobu w postaci systemu zarzadzania wymaganego jako element systemu bezpieczeństwa?

Wyjaśnienie:
Tak

17) Czy Zamawiający zgodzi się na zaklasyfikowanie wymogu możliwość automatycznego wycofania zmian w trakcie wdrażania spójnej polityki bezpieczeństwa jeśli na jednym z urządzeń nowa polityka nie zostanie poprawnie zainstalowana, jako wymagania dodatkowego którego niespełnienie nie wyklucza rozwiązania?

Wyjaśnienie:

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl

Wymaganie, aby system zarządzania urządzenia pełniącego funkcję bramy bezpieczeństwa sieciowego miało możliwość automatycznego wycofania zmian w trakcie wdrażania spójnej polityki
bezpieczeństwa jeśli na jednym z urządzeń nowa polityka nie zostanie poprawnie zainstalowana jest wymogiem dodatkowym (patrz kryteria dodatkowe na formularzu oferty).

18) Czy Zamawiający dopuszcza zastosowanie urządzenia służącego do bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym bez zastosowania Check Point SmartEvent?

Wyjaśnienie:
Zamawiający posiada rozwiązanie CheckPoint SmartEvent a postawione wymaganie w części X pkt. 2 opisu przedmiotu zamówienia jest wymaganiem dodatkowym i dotyczy tylko urządzeń, które integrują się z posiadanym rozwiązaniem.

19) Wymagania:
Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików
Czy Zamawiający dopuszcza zastosowanie rozwiązania nieposiadającego powyższych funkcjonalności?

Wyjaśnienie:
Tak, Zamawiający zgadza się, aby te wymagania były wymaganiami dodatkowymi. Zatem w części III pkt 1.13 i 1.14 zostają wykreślone. Część VIII „Zaawansowane funkcjonalności eliminacji ataków zero-day" otrzymuje brzmienie:
1. Urządzenie pełniące funkcję bezsygnaturowego wykrywania ataków zero-day poprzez analizę plików w wydzielonym środowisku wirtualnym które poza modułem umożliwiającym analizę podejrzanych plików w wydzielonym środowisku emulacyjnym, realizuje funkcję dostarczania bezpiecznych plików poprzez usunięcie z nich zawartości aktywnej.
2. Moduł dostarczania bezpiecznych plików musi wspierać co najmniej następujące formaty:
a) Pakiet Microsoft Office: doc, docm, docx, dot, dotm, dotx, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, sldm, sldx, rtf, xla, xlam, xlm, xls, xlsb, xlsm, xll, xlsx, xlt, xltm, xltx, xlw
b) Pdf, fdf
3. Proces bezpiecznego dostarczania plików musi być realizowany na co najmniej dwa sposoby:
a) Konwersja do statycznego pliku pdf
b) Usuwanie treści aktywnej i zachowanie pierwotnego formatu plików
4. Administrator musi mieć możliwość utworzenia listy adresatów oraz nadawców poczty e-mail, którzy mają być wykluczeni z inspekcji plików.

Zamawiający informuję, że udzielone wyjaśnienia są wiążące dla wszystkich Wykonawców ubiegających się o udzielenie przedmiotowego zamówienia.

Kanclerz
Politechniki Gdańskiej
mgr inż. Marek Tłok

POLITECHNIKA GDAŃSKA
ul. Narutowicza 11/12
80-233 Gdańsk
Tel.: +48 58 347 12 15
Fax.: +48 58 347 14 15
e-mail: kanclerz@pg.gda.pl
www.pg.gda.pl