Bankowy Fundusz Gwarancyjny

DAZ.261.1.2019
numer postępowania DAZ/ZP/1/2019

Warszawa, dnia 21 sierpnia 2019 r.

Do uczestników postępowania

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego, pn.: **„Dostawa i wdrożenie systemu zapór sieciowych wewnętrznych (tzw. firewall) wraz z usługą szkolenia".**

Działając na podstawie art. 38 ust. 1, 2 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2018 r., poz. 1986 z późn. zm.), zwanej dalej „ustawą Pzp", Zamawiający udziela odpowiedzi na pytania Wykonawców dotyczące Specyfikacji istotnych warunków zamówienia (SIWZ), które wpłynęły do ww. postępowania:

Pytanie nr 1:

1.19. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

Czy Zamawiający dopuści jako rozwiązanie równoważne System zabezpieczeń firewall pozwalający na tworzenie sygnatur dla nowych aplikacji za pomocą zewnętrznych narzędzi i wsparcia producenta ?

Odpowiedź:

Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.

Zamawiający nie dopuszcza rozwiązania opisanego przez Wykonawcę.

Pytanie nr 2:

3.2. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW, który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

Czy Zamawiający dopuści równoważne rozwiązanie, które uruchamia moduł filtrowania stron WWW per urządzenie? Sugerowany sposób realizacji blokowania stron WWW uniemożliwia zastosowanie rozwiązań wielu producentów, których sposób realizacji blokowania stron jest równie skuteczny do wskazanego w opisywanym punkcie. Z punktu widzenia bezpieczeństwa infrastruktury IT konfiguracja filtrowania stron WWW powinna być włączona na całym urządzeniu, a możliwość jej wyłączenia per polityka bezpieczeństwa nie jest do niczego potrzebna, a jest dodatkowo podatna na błąd ludzki.

Odpowiedź:

Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.

Zamawiający nie dopuszcza rozwiązania opisanego przez Wykonawcę.

ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa
tel. 22 58 30 700, 58 30 610, fax 22 58 30 589
e-mail: kancelaria@bfg.pl, www.bfg.pl

Pytanie nr 3:

3.4. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

Wnosimy o dopuszczenie rozwiązania równoważnego, które zapewniać będzie możliwość ręcznego tworzenia własnych kategorii filtrowania i używania ich w politykach bezpieczeństwa za pomocą zewnętrznych narzędzi producenta.

Odpowiedź:

Zamawiający zezwala na tworzenie sygnatur przy użyciu zewnętrznych narzędzi, pod warunkiem, że narzędzia te nie są pozycjami dodatkowo płatnymi (np. dostępnymi w ramach osobnej płatnej subskrypcji / licencji). Oferowane narzędzie będzie oficjalnym edytorem polecanym przez producenta.

Pytanie nr 4:

3.5. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcja. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.

Tak zdefiniowane wymaganie w zakresie ochrony dla protokołu POP3 i IMAP jest nieuzasadnione. Podane przykładowe protokoły służą jedynie do synchronizacji pomiędzy lokalną skrzynką pocztową użytkownika na urządzeniu końcowym (komputer PC) i serwerem pocztowym, na którym zlokalizowane są skrzynki użytkowników. Jest to typowa komunikacja zaufanego użytkownika wykorzystującego klienta pocztowego z jego własnym serwerem pocztowym, na którym użytkownik ten posiada zdefiniowane konto i lokalną skrzynkę pocztową. Należy zwrócić uwagę, iż jedynym protokołem, który bierze udział w komunikacji serwera pocztowego ze światem zewnętrznym w sieci Internet jest protokół SMTP. Tylko za pośrednictwem tego protokołu ma miejsce wymiana wiadomości pocztowych pomiędzy serwerami. W przypadku chęci zapewnienie ochrony dla serwera poczty odbierającego wiadomości konieczne jest zapewnienie ochrony dla protokołu na jakim ta komunikacja zachodzi, a jest nim wspominany wyżej protokół SMTP.

Wnosimy o usunięcie z tego punktu sztucznych i nieuzasadnionych technicznie wymagań dla protokołów POP3
i IMAP, co umożliwi dostosowanie wymagań Zamawiającego do rzeczywistych parametrów technicznych serwerów pocztowych mających podlegać ochronie.

Odpowiedź:

Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.

Zamawiający dodatkowo podkreśla, że przedmiotem zamówienia jest dostawa wewnętrznych zapór sieciowych.

Pytanie nr 5:

4.5. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.

Wnosimy o uproszczenie zapisu, gdzie wystarczającym będzie konieczność wykrywania ataków w ruchu tunelowanym jak to jest przyjęte przez producentów rozwiązań typu NGFW.

Odpowiedź:

Zamawiający informuje, **że dokonał w tym zakresie modyfikacji SIWZ w odpowiedziach z dnia 14 sierpnia 2019 r., przy Pytaniu nr 13** - poprzez nadanie nowego brzmienia ppkt 4.5. znajdującemu się w pkt 4 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

„System zabezpieczeń firewall musi umożliwiać wykrywanie oraz blokowania ataków w ruchu tunelowanym."

Pytanie nr 6:

6.1. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania system.

Wnosimy o dopuszczenie rozwiązania równoważnego wiodącego dostawcy rozwiązań zabezpieczeń, w którym zarządzanie systemy zabezpieczeń odbywa się za pomocą dodatkowego oprogramowania instalowanego na stacji administratora.

Odpowiedź:

Zamawiający informuje, że dopuszcza rozwiązanie, w którym funkcjonalność opisana w pkt 6.1 Opisu przedmiotu zamówienia stanowiący Załącznik nr 1 do SIWZ może być zrealizowana z poziomu centralnej konsoli zarządzania dedykowanej przez producenta firewall'a.

Pytanie nr 7:

6.5. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).

W związku z tym, iż XML nie jest standardem API oraz XML API jest specyficzną właściwością rozwiązania firmy Palo Alto Networks wnosimy o dopuszczenie innych rozwiązań wykorzystujących inne standardy niż XML i tym samym zmianę zapisu na następującą treść: „System zabezpieczeń musi być wyposażony w interfejs API będący integralną częścią systemu, za pomocą którego możliwe jest monitorowanie oraz konfiguracja urządzenia."

Odpowiedź:

Zamawiający informuje, **że dokonał w tym zakresie modyfikacji SIWZ w odpowiedziach z dnia 14 sierpnia 2019 r., przy pytaniu nr 16** - poprzez nadanie nowego brzmienia ppkt 6.5. znajdującemu się w pkt 6 cz. V Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, jak poniżej:

"System zabezpieczeń firewall musi być wyposażony w interfejs XML API lub REST API będący integralną częścią systemu zabezpieczeń, za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)."

Pytanie nr 8:

6.9. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.

Czy Zamawiający dopuści rozwiązanie równoważne w postaci zewnętrznego urządzenia tego samego producenta służące do logowania i raportowania ?

Odpowiedź:

Zamawiający informuje, że dopuści rozwiązanie, w którym funkcjonalność, opisana w ppkt 6.9 Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ, będzie realizowana przez zewnętrzny system, pod warunkiem dostarczenia przez Wykonawcę kompletnego redundantnego rozwiązania, bez konieczności wykorzystania środowiska wirtualnego lub fizycznego Zamawiającego.

Pytanie nr 9:

W odpowiedzi na pytanie 3 Zamawiający pisze, że podtrzymuje w tym zakresie zapisy SIWZ.

Czy Zamawiający zaakceptuje jako równoważne rozwiązanie, które posiada oddzielne moduły IPS i Kontroli aplikacji, każdy z tych modułów posiada własne sygnatury, administrator posiada możliwość uruchomienia modułu kontroli aplikacji oddzielnie od modułu IPS a modułu IPS oddzielnie od modułu kontroli aplikacji, a system zabezpieczeń firewall zapewnia możliwość ręcznego tworzenia sygnatur oddzielnie dla moduły kontroli aplikacji oraz oddzielnie dla modułu IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta, lecz na poziomie kodu systemu operacyjnego moduł kontroli aplikacji współpracuje z modułem IPS przy dekodowaniu protokołów, przy czym proces ten jest zupełnie transparentny jak dla administratora tak i dla użytkowników zasobów sieciowych.

Odpowiedź:

Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.

Zamawiający nie dopuszcza rozwiązania opisanego przez Wykonawcę.

Pytanie nr 10:

W odpowiedziach na pytania 7,8 oraz 9, zamawiający informuje iż podtrzymuje zapisy siwz w zakresie wymagań dotyczących wydzielenia modułu antyspyware oddzielnie od innych modułów(w tym od Modułu AntiVirus).

Wierzymy, że intencją Zamawiającego nie jest jedynie zakup urządzeń firmy Palo Alto Networks, lecz w drodze uczciwej konkurencji wyłonienie najbardziej korzystnej oferty na system NGFW, by w najlepszy sposób zabezpieczyć zasoby teleinformatyczne Zamawiającego.

Zwracamy uwagę, że żaden producent systemów NGFW poza Palo Alto Networks, nie wydziela oddzielnego modułu antispyrawe lecz ochronę antispyware posiada najczęściej w module AntiVirus (rzadziej w module IPS)

Przykład 1. Opis modułów bezpieczeństwa rozwiązań firmy Check Point

https://www.checkpoint.com/products/next-generation-firewall/

https://www.checkpoint.com/downloads/products/check-point-appliances-brochure.pdf

Przykład 2. Opis modułów bezpieczeństwa rozwiązań firmy Cisco

https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw/datasheet-c78-742480.html

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/advanced-malware-protection/solution-overview-c22-734228.html

Przykład 3: Opis modułów bezpieczeństwa rozwiązań firmy Fortinet

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGuard_Security_Services.pdf

Przykład 4: Opis modułów bezpieczeństwa rozwiązań firmy Juniper

https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf

Przykład 5: Opis modułów bezpieczeństwa rozwiązań firmy Huawei

https://e.huawei.com/en/related-page/products/enterprise-network/security/ng-firewall/usg6600/brochure/Security-usg6650-6660-6670-6680-en

Jak da się zauważyć żaden nie opisuje oddzielnego modułu Anti-Spyware lecz każdy zapewnia ochronę Anti-Spyware w modułach Anti-Virus lub IPS.

Jedynie producent Palo Alto Networks wydziela moduł Anti-Spyware

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/policy/anti-spyware-profiles

W popularnych źródłach publicznych również jest informacja iż firmy produkujące oprogramowanie antywirusowe traktują oprogramowanie typu „spyware" jako zagrożenie równie wirusom z punktu widzenia technicznego jak i prawnego. Tym samym znane firmy produkujące narzędzia antywirusowe takie jak Symantec, PC Tools, MacAfee, Sophos, Microsoft Windows Defender dodają sygnatury i metody wykrywania oprogramowania spyware do swoich narzędzi antywirusowych i nie tworzą w tym celu dodatkowego oprogramowania.

Zważając na powyższe, zwracamy uwagę, iż w obecnym brzmieniu wymagania 3.10, 3.11 oraz 3.12 mogą być spełnione wyłącznie przez rozwiązanie producenta Palo Alto Networks, co może być naruszeniem ustawy o zamówieniach publicznych.

Wnosimy zatem o dopuszczenie w punktach 3.10, 3.11 oraz 3.12 jako równoważnego rozwiązania, które zapewnia wysokiej klasy ochronę anti-spyware lecz nie wydziela oddzielnego modułu anti-spyware, a ochronę anti-spyware zapewnia jako część funkcjonalności modułu anti-wirus lub IPS i tym samym nie ma możliwości tworzenia bezpośrednio sygnatur w module anti-spyware, lecz umożliwia tworzenie sygnatur anti-spyware w module Anti-Virus lub IPS ?

Odpowiedź:

Zamawiający informuje, że nie wykluczył w pkt 3.10, 3.11 oraz 3.12 Opisu przedmiotu zamówienia stanowiącego Załącznik nr 1 do SIWZ możliwości dostarczenia rozwiązania gdzie Anti-Virus oraz Anti-Spyware nie są osobnymi modułami.

Pytanie nr 10:

W odpowiedziach na pytania 11 oraz 12, Zamawiający informuje że ze względu na zakres informacyjny przetwarzanych danych nie akceptuje rozwiązania, w którym administrator systemu nie ma możliwości podjęcia każdorazowo decyzji o przekazaniu pliku do zewnętrznego systemu SandBox.

Proszę o dopuszczenie jako równoważne, w punkach 3.20 oraz 3.21, światowej klasy rozwiązanie, które pozwala administratorowi podjęcia każdorazowo decyzji o przekazaniu pliku do zewnętrznego systemu SandBox , a również o podjęcie decyzji o wykluczeniu rodzajów plików z (np.exe, pdf, msofffice, java) z analizy systemem Sandbox, lecz rozwiązanie takie pozwala na jednoczesną pracę tylko z prywatnym lub tylko z publicznym systemem Sandbox.

Odpowiedź:

Zamawiający podtrzymuje w tym zakresie zapisy SIWZ.

Zamawiający nie dopuszcza rozwiązania opisanego przez Wykonawcę.

Powyższe odpowiedzi stanowią integralna część SIWZ i są wiążące dla Zamawiającego i Wykonawców.

Dyrektor Departamentu
Administracji i Zamówień
Lesław Fik