



KANCELARIA PREZYDENTA
RZECZYPOSPOLITEJ POLSKIEJ

Biuro Administracyjne

BA-WZP-911-42-5/10

Warszawa, dnia 15 lipca 2010 r.

wg rozdzielnika

Dotyczy: zakup wraz z dostarczeniem urządzeń do analizy i filtrowana stron internetowych dla Kancelarii Prezydenta RP – [znak sprawy 42/2010].

Szanowni Państwo,

w związku z pytaniami otrzymanymi w dniach 13 – 14 lipca 2010r., zgodnie z art. 38 ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (Dz. U. z 2007r. Nr 223, poz. 1655 z późn. zmian.), uprzejmie wyjaśniam:

Pytanie 1 - Parametr 5:

Czy chodzi o dedykowane interfejsy sieciowe, czy o dwa interfejsy użytkownika?

Odpowiedź:

Chodzi o porty pracujące w trybie monitorowania (porty span) wykorzystywane do wspierania głównych funkcjonalności urządzeń (a nie porty przeznaczone do zarządzania).

Pytanie 2 - Parametr 7

Czy istnieje lista wymaganych trapów, które mają być generowane? Jeśli tak, to prosimy o podanie.

Czy istnieje lista cech mających być dostępnymi do monitorowania? Jeśli tak, to prosimy o podanie.

Czy istnieje lista cech mających być dostępnymi do zarządzania? Jeśli tak, to prosimy o podanie?

Odpowiedź:

SNMP ma zapewnić możliwość kontrolowania parametrów pracy urządzenia i jego komponentów (także wydajności, dostępności i awarii) oraz oprogramowania. Zaproponowane rozwiązanie powinno pozwalać przynajmniej na kontrolowanie następujących parametrów: CPUUsage, RAIDStatusChange, memoryUtilization, connectivityFailure, LinkUp, LinkDown, updateFailure, highTemperature itp.

Pytanie 3 - Parametr 8:

Czy istnieje lista wymaganych alertów?

Odpowiedź:

Zamawiający wymaga aby urządzenia pozwalały zdefiniować adresy e-mail administratorów, do których będą wysyłane alerty dotyczące przynajmniej: systemu, sprzętu, aktualizacji sygnatur, pracy proxy, działania mechanizmów antymalware i antywirusowych z możliwością wyboru priorytetu alertu (odpowiadające: Informacyjne, Ostrzeżenia Krytyczne, Wszystkie).

Pytanie 4 - Parametr 20:

Czy tak skategoryzowane URL mają być automatycznie dopisywane do istniejących kategorii i trwale zapisywane?

Odpowiedź:

Zapisywanie takich URL nie jest wymagane. Jednak w takim przypadku działanie takiego mechanizmu w urządzeniu powinno być tak zoptymalizowane, aby nie wpływało na znaczne obciążenie urządzenia. Musi zostać zachowany przedział wydajności zalecany przez producenta.

Pytanie 5 - Parametr 26:

W opisie jest pewna niejasność - „Możliwość obejścia inspekcji HTTPS na podstawie wyników mechanizmów filtrowania i reputacji”. Z naszych doświadczeń wynika, że mechanizmy filtrowania mogą opierać się o zawartość, a wtedy na obejście jest cokolwiek za późno. Czy Zamawiający może podać przykład zastosowania?

Odpowiedź:

Urządzenie ma zapewniać możliwość inspekcji HTTPS. Ze względów funkcjonalnych musi istnieć mechanizm pozwalający, na podstawie zadanych parametrów, ominięcie mechanizmu inspekcji polegającej na deszyfrowaniu.

Przykłady (scenariusze użycia Zamawiającego):

Jeśli odwiedzane są strony banków, które zostały dodane do zdefiniowanej przez użytkownika kategorii URL to nie wykonywana jest inspekcja HTTPS

Jeśli stronę będącą w kategorii odwiedza użytkownik (konkretny) ze specjalnie zdefiniowanego segmentu sieci, to można zrezygnować z mechanizmu inspekcji.

Pytanie 6 - Parametr 29:

Czy urządzenie ma być stosowane jako router? Bądź całkowity ruch z wewnątrz sieci będzie nań przekierowywany „na ślepo”? Jeśli nie, to czy Zamawiający może rozwinąć opis?

Odpowiedź:

Zamawiający nie przewiduje pracy urządzenia jako routera. Preferowane zastosowanie to monitorowanie ruchu w warstwie aplikacyjnej.

Zamawiający przewiduje możliwość wykorzystania funkcjonalności w następujący sposób: Monitorowany ruch będzie przekierowany do urządzenia poprzez tzw. porty span (porty w trybie monitor) lub poprzez wpięcie urządzenia pomiędzy siecią LAN a siecią zewnętrzną i jednocześnie przed zaporą sieciową (w tym przypadku cały ruch przechodzi „na ślepo” jak to określił Pytający). Urządzenia powinny zapewniać oba tryby pracy.

Pytanie 7 - Parametr 30:

Co kryje się pod słowem „obiekty”?

Odpowiedź:

Określenie “Obiekty” odnosi się do parametru 28. Chodzi o obiekty rozróżniane przez tego typu urządzenia takie jak na przykład obiekty plikowe: audio, video, torrent, programy wykonywalne, programy pakietów biurowych.

Pytanie 8 - Załącznik nr 2 do SIWZ parametr 4:

Czy, biorąc pod uwagę opisany w SIWZ sposób podłączenia urządzeń do sieci Zamawiającego, który nie wymaga stosowania aż 6-ciu interfejsów, Zamawiający dopuszcza zaoferowanie rozwiązania z 4-ma fizycznymi interfejsami 10/100/1000 RJ45?

Odpowiedź:

Zamawiający podtrzymuje zapisy SIWZ.

Pytanie 9 - Załącznik nr 2 do SIWZ parametr 19:

Biorąc pod uwagę, że baza danych URL dostarczana przez producenta posiada ponad 90 różnych kategorii, które w większości przypadków są wystarczające do zdefiniowania polityki bezpieczeństwa dla system ochrony web, czy Zamawiający dopuszcza zaoferowanie rozwiązania, które umożliwia tworzenie do 500 własnych kategorii dodatkowo?

Uzasadnienie:

Zwracamy uwagę, że wprowadzanie dużej ilości własnych kategorii nie jest zalecane ze względu na efektywność zarządzania systemem bezpieczeństwa dla administratorów i dodatkowym utrudnieniem dla nich w razie konieczności rozwiązania problemów w komunikacji.

Odpowiedź:

Zamawiający dopuszcza zaoferowanie rozwiązania, które umożliwia tworzenie minimum 500 własnych kategorii.

Pytanie 10 - Załącznik nr 2 do SIWZ parametr 29:

Prosimy o dokładniejsze wyjaśnienie tego wymagania. Czy analizowany pod kątem malware "calling-home" ma być ruch, który trafia na dostarczone urządzenie? Zwykle w praktyce na urządzenia dla ochrony ruchu web jest przekierowany wyłącznie ruch, który może być przez nie analizowany a nie cały ruch TCP/IP na dowolnych portach. Tym bardziej, że zgodnie z innymi wymaganiami Zamawiający zakłada podłączenie w trybie transparent proxy lub explicit proxy?

Odpowiedź:

Zamawiający przewiduje wykorzystanie urządzeń poprzez wpięcie pomiędzy siecią LAN a siecią zewnętrzną i jednocześnie przed zaporą sieciową (w tym przypadku cały ruch przechodzi przez urządzenie).

Pytanie 11:

Czy zamawiający dopuszcza zmianę brzmienia zapisów §3 wzoru umowy poprzez zamianę słowa „udziela” na „przekazuje”. Paragraf 3 wzoru umowy otrzymałby następujące brzmienie:

- „1. Wykonawca przekazuje Zamawiającemu licencje na korzystanie z oprogramowania niezbędnego do zachowania funkcjonalności dostarczanych urządzeń.
2. Zamawiający zobowiązany jest do korzystania z oprogramowań zgodnie z ich przeznaczeniem i licencją producenta.
3. Licencje zostają udzielone przez Producenta na czas nieokreślony.”

Uzasadnienie:

Wykonawca nie ma uprawnień do udzielania licencji na oprogramowanie producenta, bowiem zgodnie z zapisami licencji (End User Licence Agreement) dołączanej do oprogramowania jest ona udzielana bezpośrednio przez Producenta użytkownikowi końcowemu czyli Zamawiającemu, natomiast Wykonawca jedynie przekazuje (sprzedaje) te licencje wraz ze sprzętem (oprogramowaniem) i nie jest zaangażowany jako podmiot w proces udzielania praw do korzystania z programu komputerowego. Wobec powyższego pozostawienie dotychczasowego zapisu byłoby nieuprawnione i niezgodne z prawdą, bowiem Wykonawca nie może przenieść na podmiot trzeci więcej praw niż sam posiada.

Odpowiedź:

Zamawiający wyraża zgodę na zaproponowaną powyżej zmianę zapisów § 3 umowy.

Pozostałe postanowienia specyfikacji istotnych warunków zamówienia pozostają bez zmian.

Z wyrazami szacunku

*Elżbieta Chodkiewicz
Dyrektor Biura Administracyjnego*