POLSKA AGENCJA PRASOWA S.A.

ul. Bracka 6/8, 00-502 Warszawa
tel. centr. (+48 22) 509 22 22
www.pap.pl

Warszawa, dn. 26 marca 2020 r.

DO WYKONAWCÓW

odpowiedzi na pytania złożone w postępowaniu o udzielenie zamówienia publicznego na dostawę do PAP S.A. urządzeń systemu bezpieczeństwa sieciowego typu firewall
(nr sprawy 06/20)

Zamawiający – Polska Agencja Prasowa S.A., zgodnie z art. 38 ust. 1 i 2 Ustawy z 29 stycznia 2004 r. – Prawo zamówień publicznych w odpowiedzi na pytania wykonawców złożone w przedmiotowym postępowaniu, odpowiada:

Pytanie

W odpowiedzi na pytanie z dnia 23.03.2020 Zamawiający zmienił treść wymagania I.1.15 na brzmiące:

> *„Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje profil IPS, sygnatury IPS ani dekodery protokołu IPS.”*

Jak da się zauważyć, Zamawiający jedynie w jednym miejscu zmienił treść z „moduł IPS” na „profil IPS”, pozostawił natomiast niezmienioną pozostałą cześć wymagania.

Wymaganie w obecnej postaci niestety narzuca zasadę obsługi pakietów na poziomie jądra i procesów systemu operacyjnego, gdyż wiele rozwiązań przy analizie IPS posługuje się dekoderami aplikacji lub odwrotnie, gdyż jak wiadomo, kontrola IPS polega na analizie i wykrywaniu anomalii w ruchu do konkretnej aplikacji (sygnatury IPS nie działają same z siebie tylko wyłapują ataki/anomalie przy konkretnych zidentyfikowanych aplikacjach). Stąd co najmniej w architekturze systemu operacyjnego na poziomie jądra moduły i procesy IPS muszą współpracować z modułami i dekoderami rozpoznawania(kontroli) aplikacji, a wręcz analiza IPS wykonywana już po rozpoznaniu aplikacji.

Rozumiemy, że intencją Zamawiającego jest możliwość oddzielnego sterowania profilami i politykami IPS oraz profilami i politykami kontroli Aplikacji, i dla Zamawiającego nie jest istotne jak procesy systemu operacyjnego komunikują się miedzy sobą na poziomie jądra systemu operacyjnego.

Powyższe wymaganie w połączeniu z pozostałymi umożliwia złożenie oferty wyłącznie na urządzenie Palo Alto.

Prosimy zatem o uproszczenie wymagania do postaci:

> *Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje profil IPS, sygnatury IPS.*

Odpowiedź

W ROZDZIAŁE XX pkt. I.1.15 specyfikacji przetargowej otrzymuje brzmienie:

„Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje profil IPS, sygnatury IPS."

Pytanie

W odpowiedzi na pytanie z dnia 23.03.2020 Zamawiający zmienił treść wymagania I.1.21 na brzmiące:

> *System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, gzip, hta, pdf, tar, text/html, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.*
>
> *Wymaga się aby możliwa była jednoznaczna identyfikacja plików minimum narzędzi pakietu Office takich jak Word czy Excel.*

Wymaganie w takiej postaci nadal może być spełnione tylko przez rozwiązanie Palo Alto, dlatego prosimy o dopuszczenie rozwiązania które nie wspiera plików dll w module blokowania plików, ale posiada możliwość dopisania sygnatur w np. IPS, lub ma możliwość blokowania plików na podstawie reguł regex.

Odpowiedź

W ROZDZIAŁE XX pkt. I.1.21 specyfikacji przetargowej otrzymuje brzmienie:

„System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: cab, doc, docx, ppt, pptx, xls, xlsx, rar, zip, exe, pdf, tar, text/html, pliki zaszyfrowane. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia. Wymaga się, aby możliwa była jednoznaczna identyfikacja plików minimum narzędzi pakietu Office takich jak Word czy Excel."

Pytanie

W odpowiedzi na pytanie z dnia 23.03.2020 Zamawiający udzielił odpowiedzi na pytanie dotyczące wymagania I.1.23.

Wymaganie w obecnej postaci możliwe do spełnienia tylko przez rozwiązanie Palo Alto dlatego prosimy o dopuszczenie rozwiązania alternatywnego, które posiada ochronę przed atakami dryve-by-download posiada możliwość blokowania plików, a akcja „kontynuuj" możliwa do skonfigurowania będzie wyświetlana już przy próbie wejścia na stronę z plikiem.

Odpowiedź

Zamawiający usuwa wymaganie wymienione w pkt. I.1.23.

Pytanie

Dotyczy wymagania I.2.2.

Prosimy o dopuszczenie rozwiązania obsługującego protokół RADIUS jako alternatywy dla SYSLOG.

Odpowiedź

Zamawiający dopuszcza rozwiązanie *obsługujące protokół RADIUS jako alternatywy dla SYSLOG*

Pytanie

Dotyczy wymagania I.5.3. oraz I.5.4.

W odpowiedzi na pytanie z dnia 23.03.2020 Zamawiający zmienił treść wymagania I.5.3. oraz I.5.4.dodając zapis:

> *Zamawiający dopuszcza się zmianę, w której system zarządzania realizuje dostęp na podstawie RBAC (role based access control) i pozwala na blokowanie wprowadzania i*

zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji. Wymaga się, aby w przypadku awarii systemu zarządzania prace dokonywane przez wielu administratorów miały ten sam charakter co przed awarią zatem system zarządzania dla takiego rozwiązania musi być w postaci redundantnej.

Wymaganie by tylko dla tej jednej funkcjonalności dostarczyć redundantny system zarządzania wydaje się nie mieć uzasadnienia, gdyż na czas awarii systemu zarządzania, główna funkcjonalność systemu bezpieczeństwa firewall nadal pozostaje działająca i możliwa do zarządzania i konfiguracji. Przy czym Zamawiający określił SLA na rozwiązanie awarii systemu zarządzania.

W OPZ Zamawiający do systemu zarządzania podaje bardziej krytyczne wymagania, takie jak:

13. System zarządzania, logowania i raportowania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa…

16. System zarządzania, logowania i raportowania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium

18. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.

19. System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek.

19. System zarządzania, logowania i raportowania musi umożliwiać tworzenie kopii zapasowych zarządzanych.

28. System zarządzania, logowania i raportowania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów firewalli.

Utrata jednej z powyższych funkcjonalności w przypadku awarii systemu zarzadzania może skutkować utratą możliwości zarządzania systemem firewall lub co najmniej obniżeniem poziomu ochrony zapewnianej przez system firewall, a jednak Zamawiający w tym przypadku nie wymaga redundantnego systemu zarządzania.

Stąd wydaje się, że w odpowiedzi na stawiane pytania intencją Zamawiającego było uniemożliwienie złożenia konkurencyjnej oferty w stosunku do rozwiązania Palo Alto, a nie podniesienie stabilności systemu i poziomu bezpieczeństwa chronionych zasobów.

Prosimy o dopuszczenie rozwiązania dla którego funkcjonalność będzie realizowana z poziomu systemu zarzadzania, przy czym zachowując wymaganie by system zarządzania był dostarczony jako pojedyncze urządzenie, gdyż funkcjonalność ta nie jest krytyczna z punktu widzenia poziomu bezpieczeństwa i jednocześnie Zamawiający dopuszcza pojedyncze urządzenia dla bardziej krytycznych funkcjonalności.

Odpowiedź

Zamawiający podtrzymuje dodany zapis. Sposób administrowania firewallami nie może ulec zmianie w przypadku awarii systemu zarządzania. Jeżeli system zarządzania ulegnie awarii to krytyczne funkcjonalności takie jak raportowanie, pobieranie aktualizacji, tworzenie kopii zapasowych konfiguracji, przechowywanie różnych wersji konfiguracji czy przekierowanie logów winny być przejęte przez urządzenia firewall. Jeżeli nie jest to możliwe wymaga się systemu zarządzania w postaci redundantnej.