POLSKA AGENCJA PRASOWA S.A.

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

Warszawa, dn. 20 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 punkcie nr 2.23 SIWZ (ROZDZIAŁ XX - Przedmiot zamówienia) Zamawiający określił, aby:
System zabezpieczeń firewall powinien posiadać funkcję ochrony przed atakami wykorzystującymi protokół DNS m.in. przesyłanie wykradzionych danych lub komunikacja z serwerem C&C przez DNS (DNS tuneling) oraz wykorzystanie algorytmu generowania domen (DGA)
Prosimy o wyjaśnienie, czy słowo „powinien" z tym zadaniu wg Zamawiającego wskazuje na konieczność posiadania przez system określonym w tym punkcie określonych funkcji w chwili dostarczenia systemu czy też wskazuje, aby system miał możliwość rozbudowy o tą funkcjonalność w przyszłości?

Odpowiedź

Punkt 2.23 SIWZ (ROZDZIAŁ XX - Przedmiot zamówienia) otrzymuje nowe brzmienie:
System zabezpieczeń firewall musi mieć możliwość rozbudowy poprzez zakupienie dodatkowych licencji o funkcjonalność która zapewni ochronę przed atakami wykorzystującymi protokół DNS m.in. przesyłanie wykradzionych danych lub komunikacja z serwerem C&C przez DNS (DNS tuneling) oraz wykorzystanie algorytmu generowania domen (DGA).

Pytanie

W punkcie 2.28, 2.29, 2.30, 2.31 SIWZ (ROZDZIAŁ XX - Przedmiot zamówienia) Zamawiający określił, aby:
2.28. System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, Ms-Offfice, jar, flash, apk, rar, MacOSX, Linux, JScript, PowerShell, Shell Scripts, VBScript) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 2,5 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować

system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.

2.29. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

2.30. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.

2.31. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.

Czy Zmawiający wskazuje na konieczność posiadania przez system określonych w tych punktach funkcji w chwili dostarczenia systemu? Czy też wskazuje, aby system miał możliwość rozbudowy o tą funkcjonalność w przyszłości?

Odpowiedź

Punkty 2.28, 2.29, 2.30, 2.31 SIWZ (ROZDZIAŁ XX - Przedmiot zamówienia) otrzymują nowe brzmienie:

2.28. System zabezpieczeń firewall musi mieć możliwość rozbudowy poprzez zakupienie dodatkowych licencji o funkcjonalność która zapewni możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, Ms-Offfice, jar, flash,apk, rar, MacOSX, Linux, JScript, PowerShell, Shell Scripts, VBScript) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 2,5 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.

2.29. Integracja z zewnętrznymi systemami typu "Sand-Box", po rozbudowaniu systemu poprzez zakupienie dodatkowych licencji, musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

2.30. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”, po rozbudowaniu systemu poprzez zakupienie dodatkowych licencji.

2.31. Po rozbudowaniu systemu o powyższą funkcjonalność, musi on generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.