Załącznik nr 1 do Zapytania ofertowego – Opis przedmiotu zamówienia

Przedmiotem zamówienia jest sprzedaż, dostawa, instalacja i konfiguracja systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day, z uwzględnieniem poniższych wymagań:

I. System zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day (zwany dalej „Systemem"):

1. System składa się z urządzenia dedykowanego (typu sprzętowy appliance) do pełnienia funkcji systemu zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day wraz z komponentami montażowymi do instalacji w stelażu 19".
2. Obudowa musi zawierać układ nadmiarowy dla modułów zasilania i chłodzenia umożliwiający wymianę tych elementów w razie awarii bez konieczności wyłączania Systemu.
3. Oferowany system ochrony musi umożliwiać otwarcie dostarczanego za pośrednictwem żądanych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w wirtualnym systemie operacyjnym a następnie podjęcie akcji (zablokuj/prześlij do odbiorcy) w zależności od analizy skutków otwarcia pliku w wirtualnym systemie operacyjnym.
4. System musi mieć możliwość uruchomienia co najmniej 8 wirtualnych maszyn symulujących posiadane systemy operacyjne i oprogramowanie Zamawiającego tj. Windows Xp, Windows 7, Office 2007, Office 2010, Adobe Acrobat 11. Wykonawca dostarczy system z przygotowanymi maszynami wirtualnymi. Jeśli użycie funkcjonalności wymaga posiadania licencji, licencje te zostaną dostarczone wraz z systemem.
5. Wspierane protokoły:
   - poczta: SMTP;
   - www: HTTP i HTTPS;
6. Obsługa plików MS Office, Adobe Acrobat, plików wykonywalnych, archiwów:
   - pdf Adobe acrobat document;
   - doc Microsoft Word 97-2003 Document;
   - docx Microsoft Word Document;

- xls Microsoft Excel 97-2003 Worksheet;
- xlsx Microsoft Excel Worksheet;
- ppt Microsoft PowerPoint 97-2003 Presentation;
- pptx Microsoft PowerPoint Presentation;
- exe Executable File;
- tar Tar Archive;
- zip Zip Archive;
- rar Rar Archive;
- Seven-Z 7z Archive;
- rtf Rich Text Format File;
- dot Word Template;
- docm Word macro-enabled document;
- dotx Word template;
- dotm Word macro-enabled template;
- xlt Legacy Excel 97-2003 templates;
- xlm Excel macro;
- xltx Excel template;
- xlsm Excel macro-enabled workbook;
- xltm Excel macro-enabled template;
- xlsb Excel binary worksheet;
- xla Excel add-in or macro;
- xlam Excel add-in;
- xll Excel XLL (DLL based) add-in;
- xlw Excel workspace;
- pps Legacy PowerPoint slideshow;
- pptm PowerPoint macro-enabled presentation;
- potx PowerPoint template;
- potm PowerPoint macro-enabled template;
- ppam PowerPoint add-In;
- ppsx PowerPoint slideshow;
- ppsm PowerPoint macro-enabled slideshow;
- sldx PowerPoint slide;
- sldm PowerPoint macro-enabled slide;
- csv Comma-separated values file;

7. Wspierane środowiska emulacyjne:
   - WinXP, Windows 7;
   - Office 2003, 2007, 2010;
   - Adobe 9, 11;
   - Możliwość rozbudowy o dodatkowe środowiska emulacyjne;
8. Praca w trybach sieciowych:
   - tap/mirror port;
   - in-line;
   - MTA (Mail transfer agent);
9. Praca w trybach:
   - blokowania/ochrony (prevent);
   - wykrywania/informowania (detect);
10. Praca w trybie chmury prywatnej z możliwością całkowitego wyłączenia wysyłania informacji przez Internet.
11. Wydajność i skalowalność:
   - obsługa co najmniej 700 użytkowników;
   - obsługa co najmniej 700 skrzynek pocztowych;
   - sandboxing co najmniej do 250 000 tysięcy plików miesięcznie;
   - możliwość rozbudowy chmury prywatnej o dodatkowe urządzenia;
12. Scentralizowane zarządzanie konfiguracją, polityką i logami. Zarządzanie systemem musi zostać dostarczone w ramach niniejszego postępowania lub dostarczone rozwiązanie musi być zarządzane z posiadanego przez Zamawiającego systemu zarządzania Check Point SmartCenter.
13. System zarządzania musi zapewniać korelację zdarzeń generowanych przez system zapobiegania i wykrywania zagrożeń zamaskowanych, nierozpoznanych i zagrożeń typu zero-day ze zdarzeniami generowanymi przez posiadany przez Zamawiającego system zapór sieciowych Check Point Security Gateway. System korelacji musi zostać dostarczony w ramach niniejszego postępowania lub dostarczone rozwiązanie musi współpracować z posiadanym przez Zamawiającego systemem korelacji zdarzeń Check Point SmartEvent.
14. Dopuszcza się zastosowanie dwóch urządzeń typu sprzętowy appliance, jednego dla ruchu SMTP, drugiego dla ruchu WWW z zapewnieniem jednego scentralizowanego zarządzania dla obu urządzeń.

15. Dostarczone urządzenie musi być produktem fabrycznie nowym dostarczonym przez autoryzowany kanał sprzedaży.

II. Usługi:

W ramach instalacji i konfiguracji Wykonawca:

1. Podłączy dostarczony sprzęt do infrastruktury Zamawiającego. Jeśli wymagane będą zmiany konfiguracji oprogramowania Zamawiającego, Wykonawca dokona analizy i wprowadzi niezbędne zmiany.
2. Dostarczy dokumentację operatora/administratora/użytkownika systemu w języku polskim lub angielskim. Dokumentacja musi zawierać informacje pozwalające na samodzielną konfigurację i administrację dostarczonego Systemu.

III. Warunki gwarancji:

1. System musi być objęta gwarancją producenta na sprzęt jak i oprogramowanie przez okres co najmniej 1 roku. Gwarancja ma być świadczona co najmniej w trybie 5x9 z czasem reakcji co najwyżej 4 godziny od chwili dokonania zgłoszenia przez Zamawiającego.
2. Gwarancja będzie świadczona przez Wykonawcę w oparciu o gwarancje producenta.
3. Zgłaszanie awarii dokonywane będzie pisemnie, faksem lub pocztą elektroniczną w godzinach pracy Zamawiającego.
4. Wykonawca przystąpi do naprawy w miejscu instalacji sprzętu w siedzibie Zamawiającego.
5. Jeśli naprawa w siedzibie Zamawiającego nie jest możliwa, Wykonawca będzie ją realizował na zewnątrz. W przypadku realizacji naprawy na zewnątrz koszty transportu ponosi Wykonawca.
6. W przypadku uszkodzenia urządzenia Wykonawca dokona jego naprawy bądź wymiany na nowe w ciągu 5 dni roboczych od chwili dokonania zgłoszenia przez Zamawiającego. Naprawa i wymiana musi obejmować swoim zakresem wszelkie prace konfiguracyjne niezbędne do poprawnego działania Systemu.

7. W przypadku nieprawidłowego działania Systemu Wykonawca dokona jego naprawy w ciągu jednego dnia roboczego od chwili dokonania zgłoszenia przez Zamawiającego.
8. W przypadku uszkodzenia urządzenia bądź nieprawidłowego działania Systemu, trwającego dłużej niż jeden dzień roboczy, Wykonawca, najpóźniej w drugim dniu roboczym trwania awarii, wykona w siedzibie Zamawiającego niezbędne prace konfiguracyjne mające na celu zapewnienie poprawnego działania systemu pocztowego oraz innych systemów zależnych Zamawiającego.
9. W ramach gwarancji Wykonawca będzie świadczył usługi konsultacji technicznej w terminach ustalanych w trybie roboczym.
10. Konsultacje techniczne będą realizowane drogą telefoniczną i elektroniczną.
11. W ramach gwarancji Wykonawca zapewni dostęp do poprawek i nowych wersji oprogramowania wbudowanego w dostarczony system przez okres trwania gwarancji.