ZP-3710-9/13

**Specyfikacja istotnych warunków zamówienia**
**na zakup sprzętu teleinformatycznego**
**dla Krajowego Biura Wyborczego**

**Ogłoszenie zostało wysłane do Biuletynu Zamówień Publicznych z numerem: 246223-2013**

**Zamówienie zostanie udzielone w trybie przetargu nieograniczonego** (art. 39 - art. 46 Prawa zamówień publicznych).

**Zamawiający:**
Krajowe Biuro Wyborcze w Warszawie, ul. Wiejska 10, 00-902 Warszawa.

**Adres strony internetowej, na której znajduje się specyfikacja zamówienia**
www.pkw.gov.pl/zamówienia publiczne

**Przedmiot zamówienia:**

Dostawa urządzeń telekomunikacyjnych spełniających funkcje:

1. Wielozadaniowy system zabezpieczeń sieciowych wraz z wdrożeniem i wsparciem technicznym — 4 szt. (2 klastry)
2. System do wykrywania, identyfikacji i oceny podatności systemów na incydenty sieciowe — 1 szt.
3. Programowego systemu do ochrony przed atakiem DDoS (zakłócającym ciągłość pracy udostępnianych usług) — 1 szt.
4. Licencje na program antywirusowy do poczty elektronicznej na 8 tysięcy kont pocztowych.

Minimalne wymagania techniczne i funkcjonalne dotyczące poszczególnych pozycji zawiera Załącznik Nr 1 do niniejszej specyfikacji.

**Miejsce dostaw:**
Krajowe Biuro Wyborcze, ul. Wiejska 10.

**Szczególne warunki wykonania zamówienia**
Nie dopuszcza się zamówień częściowych.
Nie dopuszcza się do złożenia ofert wariantowych.

**Termin wykonania zamówienia.**
Dostawa sprzętu do miejsca dostawy —21 dni od dnia podpisania umowy.

**Warunki udziału w postępowaniu oraz informacje o oświadczeniach i o dokumentach jakie mają dostarczyć Wykonawcy.**
O udzielenie zamówienia mogą ubiegać się Wykonawcy spełniający warunki określone w art. 22 Prawa zamówień publicznych i nie podlegający wykluczeniu z przyczyn wskazanych w art. 24 tej ustawy. Wykonawcy wraz z ofertą obowiązani są złożyć pisemne oświadczenia o spełnieniu ww. warunków, stanowiącym Załącznik Nr 2 do niniejszej specyfikacji.

**Wadium**
Bez wadium

**Kryteria oceny ofert i ich znaczenie**
Wśród złożonych w terminie ofert spełniających określone w SIWZ wymagania dotyczące urządzeń telekomunikacyjnych jedynym **kryterium wyboru oferty będzie najniższa cena.**

**Termin związania ofertą.**
Wykonawcy są związani ofertą przez 60 dni. Bieg terminu związania ofertą rozpoczyna się z upływem terminu składania ofert.

**Sposób porozumiewania się Zamawiającego z Wykonawcami oraz wskazanie osoby uprawnionej do porozumiewania się z Wykonawcami w imieniu Zamawiającego.**

1. Oświadczenia, wnioski, zawiadomienia oraz informacje i pytania Zamawiający i Wykonawcy przekazują pisemnie lub faksem. Dokumenty przekazane faksem uważa się za złożone w terminie, jeśli ich treść dotarła do adresata przed upływem terminu i została niezwłocznie potwierdzona pisemnie.
2. Do porozumiewania się z Wykonawcami w imieniu Zamawiającego jest upoważniony:
   a) pod względem merytorycznym:
      Romuald Drapiński – pok. nr 419, tel. 022 695-26-36, w godz. 9.00–16.00
      Grzegorz Rogaczewski – pok. nr 319, tel. 022 695-24-15, fax. 022 625-36-87, w godz. 9.00–16.00
   b) pod względem formalnym:
      Marek Mazur – pok. nr 316, tel. 022 695-24-16, w godz. 9.00–16.00.

**Miejsce i termin składania ofert.**

**1.** Oferty należy składać w zapieczętowanej kopercie. Na kopercie należy umieścić odcisk pieczęci firmy składającej ofertę oraz umieścić napis:

***Oferta na zakup urządzeń telekomunikacyjnych***
***dla Krajowego Biura Wyborczego***
***Nie otwierać do 28 listopada 2013 r.***

2. Oferty należy składać do dnia 28 listopada 2013r. do godz. 11.00 w siedzibie Krajowego Biura Wyborczego w Warszawie, ul. Wiejska 10 (gmach Kancelarii Prezydenta RP, wejście D), pok. nr 314 – Kancelaria Krajowego Biura Wyborczego, tel. 22 625-58-18.

**Sposób przygotowania oferty.**

1. Oferta musi być sporządzona na piśmie. Formularz ofertowy, stanowi Załącznik Nr 3 do niniejszej specyfikacji, ma być podpisany odręcznie czytelnie pełnym imieniem i nazwiskiem przez osobę mającą prawo do podejmowania zobowiązań w imieniu Wykonawcy (z uwzględnieniem art. 230 Kodeksu Spółek Handlowych). Osoba podpisująca ofertę parafuje każdą stronę oferty. W przypadku podpisania oferty przez osobę nie wymienioną w rejestrze handlowym lub nie będącą właścicielem do oferty

powinno zostać dołączone pełnomocnictwo (oryginał lub poświadczona notarialnie kopia).
2. Do oferty należy dołączyć oświadczenie o spełnieniu warunków określonych w art. 22 ust. 1 i art. 24 Prawa zamówień publicznych; wzór oświadczenia stanowi Załącznik nr 2 do niniejszej specyfikacji.
3. Oferta musi zawierać ostateczną, łączną wyrażoną w złotych polskich cenę jednostkową brutto i cenę brutto (łącznie z podatkiem VAT), obejmującą wszystkie związane z tym koszty.
4. Oferta powinna zawierać imię i nazwisko oraz nr telefonu i faksu osoby, która będzie udzielać odpowiedzi na pytania Zamawiającego i przyjmować informacje i dokumenty, a także będzie uprawniona do dokonywania roboczych uzgodnień związanych z realizacją zamówienia, przy zachowaniu warunków określonych w umowie.
5. Jeden Wykonawca może złożyć tylko jedną ofertę i podać tylko jedną cenę.

**Informacje o ewentualnym sposobie udzielenia dodatkowych wyjaśnień dotyczących specyfikacji.**

1. Wykonawcy zainteresowani wykonaniem zamówienia mogą zwracać się o wyjaśnienia dotyczące wątpliwości lub niejasności związanych z niniejszą specyfikacją, kierując do Zamawiającego wniosek o wyjaśnienia w terminie nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert; dopuszcza się formę elektroniczną na e-mail: gr@kbw.gov.pl, w godz. 9:00 – 16:00
2. Przekazywanie Wykonawcom informacji związanych z postępem przetargu za pośrednictwem stron internetowych www.pkw.gov.pl/zamówienia publiczne pod przedmiotowym przetargiem.
2. Zamawiający nie będzie odpowiadał na pytania Wykonawców sugerujące lub proponujące jakiekolwiek zmiany w przedmiocie zamówienia objętym specyfikacją.
3. Pisemna odpowiedź zostanie niezwłocznie przesłana wszystkim uczestnikom postępowania bez wskazania źródła zapytania.

**Otwarcie ofert.**

1. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę jaką zamierza przeznaczyć na sfinansowanie zamówienia. Otwarcie ofert nastąpi 28 listopada 2013r. do godz. 11.10 w siedzibie Krajowego Biura Wyborczego.
2. Zamawiający po otwarciu ofert w obecności oferentów przekaże informację o firmach (podając ich nazwy i adresy) oraz ceny za wykonanie zamówienia.
3. Zamawiający powiadomi pisemnie oferentów o dokonanym wyborze oferty, wskazując nazwę i adres firmy, której ofertę wybrano i cenę.
4. Zamawiający będzie pisemnie lub faksem (potwierdzonym pisemnie) powiadamiał wszystkich oferentów o odrzuceniu ofert lub wykluczeniu Wykonawców, oraz o unieważnieniu postępowania lub modyfikacji istotnych warunków zamówienia.

**Istotne dla stron postanowienia, które zostaną wprowadzone do umowy.**

1. Umowa będzie zawarta w siedzibie Zamawiającego co najmniej 5 dnia od daty zawiadomienia o wyborze Wykonawcy. Jej treść określi warunki wykonania zamówienia zgodne z niniejszą specyfikacją. Projekt umowy spełniającej warunki określone w specyfikacji przygotuje Wykonawca usługi.
2. W umowie zostanie ustalone, iż należność za sprzęt Zamawiający zapłaci po dostarczeniu sprzętu w terminie 14 dni od dnia przyjęcia faktury przez Zamawiającego. W razie

opóźnienia w zapłacie Wykonawcy będą przysługiwały odsetki ustawowe od Zamawiającego.

3. W umowie zostanie określona kara za opóźnienie w dostarczeniu sprzętu w stosunku do terminu wskazanego w umowie, w wysokości 1% wartości umowy za każdy dzień opóźnienia. Jeśli opóźnienie przekroczy 7 dni w stosunku do tego terminu, to niezależnie od kary za opóźnienie Zamawiający może odstąpić od umowy i zlecić wykonanie zamówienia innemu podmiotowi.
4. Wynagrodzenie przysługujące Wykonawcy za dostarczenie sprzętu teleinformatycznego sprzedanego przed odstąpieniem od umowy z podanych wyżej przyczyn nie może przekroczyć ceny określonej w umowie, na którą udzielono zamówienia, pomniejszonej o karę umowną i o cenę dokończenia wykonania zamówienia przez nowego Wykonawcę, z uwzględnieniem podwyższonych kosztów spowodowanych wykonaniem tego zamówienia oraz innych wydatków poniesionych przez Zamawiającego w związku ze zmianą Wykonawcy.

**Pouczenie o środkach ochrony prawnej.**

1. Wobec czynności Zamawiającego: wyboru trybu udzielenia zmówienia, opisu sposobu oceny spełniania warunków udziału Wykonawców w postępowaniu, wykluczenia Wykonawcy z postępowania lub odrzucenia oferty Wykonawcy — Wykonawcy przysługuje prawo wniesienia odwołania do Prezesa Krajowej Izby Odwoławczej w terminie 5 dni od dnia, w którym Wykonawca powziął lub mógł powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia.
2. W przypadku wniesienia odwołania na inne czynności Zamawiającego, Wykonawca może w terminie przewidzianym na wniesienie odwołania poinformować Zamawiającego o stwierdzonym uchybieniu.

Załączniki:

Załącznik Nr 1 — Minimalne wymagania techniczne i funkcjonalne przedmiotu zamówienia.
Załącznik Nr 2 — Wzór oświadczenia o spełnianiu warunków art. 22 ust. 1 i art. 24 ustawy Prawo Zamówień publicznych.
Załącznik Nr 3 — Wzór formularza ofertowego.

**Załącznik Nr 1**

## 1. Wielozadaniowy system zabezpieczeń sieciowych wraz z wdrożeniem i wsparciem technicznym

W ramach postępowania muszą zostać dostarczone cztery kompletne, gotowe do pracy urządzenia pracujące w parach jako dwa klastry (oddzielne lokalizacje sieciowe). Wraz z produktami wymagane jest dostarczenie opieki technicznej ważnej przez okres 3 lat. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz jego autoryzowanego polskiego przedstawiciela, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, aktualizację bazy ataków IPS, definicji wirusów, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Cena ma zawierać koszty wdrożenia systemu.

Właściwości wielozadaniowego systemu zabezpieczeń sieciowych:

1. System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze sprzętowej systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
3. Urządzenie zabezpieczeń musi posiadać przepływność w ruchu full-duplex nie mniej niż 2 Gb/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 1 Gb/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 250 000 jednoczesnych połączeń.
4. System zabezpieczeń musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
5. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność urządzenia zabezpieczeń przy włączonej identyfikacji aplikacji w ruchu full-duplex musi być nie mniejsza niż 2 Gb/s.
6. Urządzenie zabezpieczeń musi być wyposażone w co najmniej 12 portów Ethernet 10/100/1000. Musi być możliwość zamontowania w urządzeniu minimum 8 interfejsów optycznych (SFP).
7. System zabezpieczeń musi działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych. Musi istnieć możliwość jednoczesnej

konfiguracji i pracy poszczególnych interfejsów sieciowych w różnych trybach w pojedynczej instancji systemu zabezpieczeń.

8. Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
9. Urządzenie musi mieć możliwość pracy w trybie transparentnym L1 (bez konieczności nadawania adresu IP) oraz pozwalać na tworzenie transparentnych subinterfejsów, które będą obsługiwały ruch z wybranych vlanów lub podsieci IP.
10. Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tabela routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
11. System zabezpieczeń musi realizować zadania kontroli dostępu (filtracji ruchu sieciowego), wykonując kontrolę na poziomie warstwy sieciowej, transportowej oraz aplikacji.
12. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa). Polityki muszą być definiowane pomiędzy określonymi strefami bezpieczeństwa.
13. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
14. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
15. System zabezpieczeń musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
16. System zabezpieczeń musi umożliwiać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
17. System zabezpieczeń musi identyfikować co najmniej 1700 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS, nie mniej niż: Skype, Gada-Gadu, Tor, BitTorrent, eMule.
18. System zabezpieczeń musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.

19. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama.
20. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
21. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
22. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
23. System zabezpieczeń musi umożliwiać zarządzanie, kontrolę i wgląd w ruch nierozpoznany przez urządzenie.
24. System zabezpieczeń musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
25. System zabezpieczeń musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
26. System zabezpieczeń musi umożliwiać blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
27. Urządzenie zabezpieczeń musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznego systemu typu „Sand-Box" plików wykonywalnych (exe, dll) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 1 Gb/s w celu ochrony przed zagrożeniami typu zero-day. System zewnętrzny, na podstawie przeprowadzonej analizy, musi aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
28. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, oba), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box".
29. Administrator musi mieć możliwość dostępu do systemu analizy plików wykonywalnych w celu sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
30. System zabezpieczeń musi umożliwiać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
31. System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności

dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.

32. System zabezpieczeń musi posiadać możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
33. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
34. System zabezpieczeń musi posiadać możliwość automatycznego pobierania listy stron WWW z zewnętrznego systemu w określonych przedziałach czasu i używania ich w politykach bezpieczeństwa.
35. System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
36. System zabezpieczeń musi posiadać możliwość uruchomienia modułu inspekcji antywirusowej per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
37. System zabezpieczeń musi posiadać możliwość uruchomienia modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
38. System zabezpieczeń musi posiadać możliwość uruchomienia modułu IPS/IDS per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
39. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
40. System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
41. System zabezpieczeń musi posiadać możliwość uruchomienia modułu anty-spyware per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcjonalność anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
42. System zabezpieczeń musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

43. System zabezpieczeń musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
44. System zabezpieczeń musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
45. System zabezpieczeń transparentnie ustala tożsamość użytkowników sieci (integracja z Active Directory, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) precyzyjnie definiuje prawa dostępu użytkowników do określonych usług sieci i jest utrzymana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie. Ponadto system musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
46. System zabezpieczeń musi umożliwiać integrację funkcjonalności mapowania nazw użytkowników do używanych adresów IP z rozwiązaniami niestandardowymi (np. kontrolerami sieci WiFi) za pomocą dostępnego interfejsu API.
47. Interfejs API musi być integralną częścią systemu zabezpieczeń umożliwiającą konfigurowanie i sprawdzanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
48. 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 systemem.
49. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
50. System zabezpieczeń musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS i Kerberos.
51. System musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
52. System zabezpieczeń musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
53. System zabezpieczeń zapewnia możliwość bezpiecznego zdalnego dostępu do chronionych zasobów w oparciu o standard SSL VPN bez konieczności stosowania dodatkowych licencji.
54. System zabezpieczeń musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
55. Urządzenie zabezpieczeń musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 100 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.

56. Nie jest dopuszczalne rozwiązanie, gdzie włączenie logowania na dysk może obniżyć wydajność urządzenia.
57. Urządzenie musi mieć możliwość korelowania zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
58. Urządzenie musi mieć możliwość tworzenia wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
59. Urządzenie musi mieć możliwość stworzenia raportu o aktywności wybranego użytkownika na przestrzeni kilku ostatnich dni.
60. Urządzenie musi mieć możliwość generowania raportu na temat aktywności sieci typu Botnet wykrywanych przez system zabezpieczeń.
61. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
62. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

Zamawiający zastrzega sobie prawo do weryfikacji spełnienia jakiejkolwiek z wymienionych poniżej właściwości systemu zabezpieczeń sieciowych.

********

2. **System do badania podatności systemów sieciowych i serwerów** na incydenty sieciowe poprzez: wykrywanie, identyfikację, ocenę podatności (Vulnerability Assessment) oraz zarządzania wiedzą o wykrytych lukach (Vulnerability Management) wraz z wdrożeniem oraz wsparciem technicznym producenta na okres 3 lat.

**Wymagania funkcjonalne:**

1. Wykrywanie urządzeń obecnych w sieci - identyfikacja systemów operacyjnych; standardową funkcją powinno być skanowanie portów.
2. Identyfikowanie podatności - sieci, usług, systemów, w tym aplikacji web i baz danych.
3. Tworzenie exploitów i próby dostępu do wybranych zasobów sieci
4. System powinien umożliwiać wybór poziomu „inwazyjności" skanowania w celu uniknięcia destabilizacji badanych systemów.
5. Wykryte podatności powinny podlegać klasyfikacji wg poziomu stwarzanego zagrożenia („krytyczna", „wysoka", itp.); użytkownik powinien mieć możliwość ręcznej „zmiany" automatycznie kwalifikowanych podatności; osobno klasyfikowaną kategorię podatności powinna stanowić kategoria „false-positive", która powinna być wyłączona z raportów.
6. Wykryte podatności można opatrywać komentarzem, który zostanie automatycznie

przeniesiony do raportów; komentarz taki może być (w zależności od decyzji użytkownika) uwzględniany w przyszłych skanowaniach.
7. Korelowanie zidentyfikowanych zdarzeń.
8. Raportowanie o podatnościach i zagrożeniach
9. System powinien udostępniać raporty w dwóch trybach:
10. raport pełny
11. raport różnicowy - zawierający jedynie te informacje, które nie znalazły się w poprzednich wynikach skanowania
12. Raporty muszą być generowane co najmniej w formatach: PDF, CPE, HTML, LaTeX, NBE, TXT, XML
13. Dla raportów powinny być dostępne dwie opcje szczegółowości: streszczenia i raport pełny (raporty w formatach: "Executive" i "Detailed")
14. System musi bazować na otwartych standardach, w szczególności:
    a. SCAP (Security Content Automation Protocol)
    b. CVE (Common Vulnerabilities and Exposure)
    c. CPE (Common Platform Enumeration)
    d. CVSS (Common Vulnerability Scoring System)
    e. OVAL (Open Vulnerability and Assessment Language)

**Licencjonowanie**:

1. Licencja nie może ograniczać maksymalnej liczby adresów IP podlegających analizie, dopuszczalne jest jedynie ograniczenie liczby adresów IP badanych w jednym przebiegu skanowania, limit taki nie powinien być mniejszy niż 300 adresów
2. Licencja powinna być kompletna tj. obejmować moduł skanujący oraz konsolę zarządzająco-raportującą

**Wymagania pozostałe:**

1. Producent udostępnia pełną dokumentację systemu, dokumentację API, oraz wiedzę niezbędną do zarządzania systemem
2. System zabezpieczeń musi być dostarczony jako obraz maszyny wirtualnej na platformę VMWare Esxi
3. Konsola zarządzajaca powinna być dostępna jako aplikacja WWW, wymagane jest także zarządzanie przez CLI oraz dedykowane API; dodatkowo (ale nie zamiennie) dopuszczalne jest zarządzanie poprzez dedykowana aplikację pracującą w środowisku Microsoft Windows XP/Vista/7
4. Wraz z systemem powinno zostać zaoferowane wsparcie producenta, aktywne przez okres 3 lat od zakupu i obejmujące: subskrybcję procedur i wzorców testowych; pomoc w rozwiązywaniu problemów, wsparcie dla sprzętu i oprogramowania.

********

**3. Programowy system do ochrony przed atakiem DDoS wraz z wdrożeniem, ze wsparciem technicznym na 1 rok.**

Właściwości systemu do zabezpieczeń przed atakami DDoS

4. System zabezpieczeń musi być dostarczony jako obraz maszyny wirtualnej na

platformę VMWare Esxi.

5. Oprogramowanie musi być dostarczane i wspierane przez jednego producenta.
6. System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych serwerów w sieci wewnętrznej.
7. System zabezpieczeń musi zapewniać przepływność nie mniejszą niż 1 Gbps.
8. System zabezpieczeń musi zapewniać ochronę przed atakami DDoS dla przepływności nie mniejszej niż 1Gbps.
9. System musi być implementowany online oraz musi być na niego przekierowany cały ruch który ma być sprawdzany pod kątem potencjalnych ataków DDoS.
10. System zabezpieczeń musi działać w trybie transparentnym (bridge L2).
11. Funkcjonując w trybie transparentnym system zabezpieczeń nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych filtrujących ruch przychodzący i wychodzący.
12. System zabezpieczeń musi posiadać odrębny dedykowany interfejs sieciowy służący do zarządzania.
13. System musi być zarządzany przez linię komand (CLI) oraz przez interfejs graficzny (GUI). Dostęp do interfejsu graficznego musi być realizowany poprzez https.
14. System zabezpieczeń musi posiadać odrębny dedykowany interfejs sieciowy służący do wymiany danych w ramach klastra wysokiej dostępności HA.
15. System zabezpieczeń musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive.
16. System zabezpieczeń musi chronić przed atakami DDoS tylko na podstawie analizy ruchu przesyłanego od i do chronionych serwerów. Nie dopuszcza się instalacji jakiegokolwiek oprogramowania typu agent na chronionych serwerach.
17. System zabezpieczeń musi w czasie rzeczywistym analizować cały ruch przychodzący i wychodzący z chronionych zasobów i przy wykorzystaniu algorytmu behawiorystyczno-heurystycznego podejmować decyzję o blokowaniu ataków DDoS.
18. Nie dopuszcza się aby do ochrony serwerów i aplikacji wykorzystywane były sygnatury znanych ataków DDoS.
19. System musi dokonywać ciągłej analizy całego ruchu, zarówno przychodzącego jak i wychodzącego przy pomocy silnika statefull inspection, w celu ochrony przed atakami DDoS. Nie dopuszcza się aby system analizował statystycznie tylko część ruchu.
20. System musi dynamicznie ustalać próg dostępności danego zasobu poprzez pomiar czasów odpowiedzi chronionego serwera i aplikacji.
21. System musi przypisywać ocenę zachowania dla poszczególnych adresów IP na podstawie ruchu generowanego do chronionych zasobów. System musi przechowywać ocenę zachowania danych adresów IP przez ostatnie 30 dni.
22. System musi przydzielać dostęp do chronionych zasobów poprzez porównanie oceny zachowania użytkownika oraz progu dostępności dla danego zasobu który jest tworzony w sposób dynamiczny na podstawie obciążenia poszczególnych zasobów.
23. System zabezpieczeń musi automatycznie wykrywać serwery, które mają być przez niego chronione i samoistnie dodawać je do konfiguracji.
24. System zabezpieczeń musi mieć możliwość podziału na odrębne wirtualne instancje. W ramach każdej z instancji administrator ma możliwość definiowania chronionych adresów IP serwerów, administratorów mających dostęp do konfiguracji danej wirtualnej instancji, trybu działania rozwiązania: nauka lub aktywna ochrona.
25. System zabezpieczeń musi zapewniać ochronę przed atakami DDoS dla warstwy 7 modelu ISO/OSI (warstwa aplikacji) dla co najmniej takich usług jak http, dns i sip.
26. System zabezpieczeń musi mieć możliwość pracy w co najmniej dwóch trybach: nauki

i aktywnej ochrony. W trybie nauki system loguje filtrowany ruch, bez aktywnego blokowania ataków DDoS. W trybie aktywnej ochrony system loguje cały ruch i aktywnie chroni zasoby przed atakami DDoS.

27. System musi ograniczać do minimum liczbę fałszywych alarmów (false positive) zapewniając ochronę przed atakami DDoS tylko i wyłącznie wtedy kiedy serwery są nadmiernie obciążone.
28. System zabezpieczeń musi mieć możliwość konfiguracji białej listy dla adresów IP, które nie mają być sprawdzane przez system.
29. System zabezpieczeń musi mieć możliwość konfiguracji białej listy dla państw, które nie mają być sprawdzane przez system.
30. System musi mieć możliwość rozróżnienia ruchu generowanego przez użytkowników od ruchu maszynowego (np. pochodzącego od botnetów).
31. System musi mieć możliwość współdzielenia informacji o wykrytych atakach pomiędzy innymi instancjami tego samego typu znajdującymi się w sieci Klienta.
32. System musi w sposób automatyczny umieszczać na tymczasowej czarnej liście adresy IP hostów które wygenerowały ruch przekraczający skonfigurowane przez administratora progi.
33. System zabezpieczeń musi automatycznie usuwać adresy IP z tymczasowej czarnej listy jeśli będą one nieaktywne w ciągu ostatnich pięciu minut.
34. Administrator musi mieć również możliwość usuwania poszczególnych adresów IP z tymczasowej czarnej listy w sposób manualny.
35. Administrator musi mieć możliwość ręcznego zwiększenia wartości oceny zachowania dla poszczególnych adresów IP lub całych krajów.
36. Rozwiązanie musi mieć możliwość rozpoznawania z którego kraju i systemu autonomicznego (AS) został zainicjowany badany ruch.
37. Administrator musi mieć możliwość dodania do czarnej listy poszczególnych adresów IP, numerów systemów autonomicznych (AS) oraz krajów, powodując blokadę ruchu z nich pochodzącego.
38. System musi być w pełni kompatybilny z IPv6.
39. Rozwiązanie musi mieć możliwość wysyłania SNMP Trap.
40. Rozwiązanie musi mieć możliwość wysyłania logów do zewnętrznego serwera Syslog.
41. Rozwiązanie musi mieć możliwość wysyłania komunikatów w oparciu o protokół NetFlow.
42. System musi mieć możliwość zapisywania całego ruchu sieciowego (packet capture). System musi mieć możliwość generowania co najmniej dziewięciu różnych zrzutów pakietów w oparciu o parametry takie jak: adres IP, protokół, port.
43. Rozwiązanie musi mieć możliwość generowania raportów statystycznych bezpośrednio w systemie. Raporty muszą być generowane dla całego sytemu lub dla wybranych chronionych zasobów.

********

4. **System antywirusowy.** Zintegrowany z serwerem poczty elektronicznej Axigen 8.1.1 dla 8 tysięcy kont pocztowych — wsparcie na 3 lata.

********

**Załącznik nr 2**

**Oświadczenie o spełnianiu warunków art. 22 ust. 1 i art. 24 ust. 1 i 2**
zgodnie z ustawą z dnia 29 stycznia 2004 roku Prawo zamówień publicznych
(Dz. U. z 2010 r. nr 113, poz. 759 z późn. zmianami)

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego na dostawę urządzeń telekomunikacyjnych dla Krajowego Biura Wyborczego, zgodnie z przedmiotem zamówienia zawartym w specyfikacji istotnych warunków zamówienia do przetargu nieograniczonego ZP-3710-9/13:
ja ..... zamieszkały w .....
reprezentując firmę .....
z siedzibą w ..... przy ....., jako - wpisany w Krajowym Rejestrze Sądowym Nr KRS ..... w imieniu reprezentowanej przeze mnie firmy oświadczam, że:

1) posiadamy uprawnienia do wykonywania określonej działalności lub czynności, jeżeli ustawy nakładają obowiązek posiadania takich uprawnień (art. 22 ust.1 pkt.1),
2) posiadamy wiedzę i doświadczenie (art. 22 ust.1 pkt.2),
3) dysponujemy odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia (art. 22 ust.1 pkt.3),
4) znajdujemy się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia (art. 22 ust.1 pkt.4),
5) brak podstaw do wykluczenia nas z postępowania o udzielenie zamówienia (art. 24 ).

Ponadto, oświadczam, że zapoznaliśmy się ze wszystkimi warunkami specyfikacji istotnych warunków zamówienia.

Nasza oferta odpowiada warunkom specyfikacji i jest ważna przez okres związania ofertą określony przez Zamawiającego.

Warszawa, dnia ..... r.

.....
Podpis osoby/osób upoważnionych do reprezentowania Wykonawcy

**Załącznik nr 3**

Pieczęć Oferenta

# OFERTA

Nazwa oferenta: **.....**
Siedziba oferenta: **.....**
Uprawniony do reprezentowania wykonawcy, do kontaktów z Zamawiającym (w tym do udzielania odpowiedzi na pytania Zamawiającego), do zawarcia umowy i realizacji zamówienia :
imię ..... nazwisko ..... tel./fax: .....
Nazwa i siedziba Zamawiającego: **.....**
**.....**

**Przystępując do postępowania w sprawie ZP-3710-9/13 na udzielenia zamówienia publicznego na dostawę urządzeń telekomunikacyjnych dla Krajowego Biura Wyborczego, zgodnie ze specyfikacją istotnych warunków zamówienia, przedstawiamy ofertę o następujących cenach jednostkowych/całkowitych:**

| Lp. | Rodzaj | Szt. | Cena jedn. brutto | cena brutto |
|---|---|---|---|---|
| **1** | System zabezpieczeń sieciowych | 4 | | |
| **2** | System wykrywania podatności na incydenty | 1 | | |
| **3** | System ochrony przed DDoS | 1 | | |
| **4** | Program antywirusowy | 1 | | |
| | | | — | |
| | **Razem** | — | — | |

Oświadczam, że uważamy się za związanych niniejszą ofertą przez okres wskazany przez Zamawiającego.
W razie wybrania naszej oferty, zobowiązujemy się do podpisania umowy z uwzględnieniem zaproponowanych danych ofertowych, w terminie i miejscu określonym przez Zamawiającego.

**Załączniki stanowiące integralną część oferty:**

1. Oświadczenie o spełnianiu warunków art. 22 ust. 1 Prawa zamówień publicznych

Warszawa, dnia ..... r. ……
Podpis osoby/osób upoważnionych do reprezentowania