Załącznik nr 1 do SIWZ

numer sprawy: 7/SISP-2/PN/2014

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest rozbudowa Systemu bezpieczeństwa informatycznego GUS na potrzeby projektu System Informacyjny Statystyki Publicznej (SISP-2) polegająca na:

1. dostawie wraz z wdrożeniem systemu bezpieczeństwa sieciowego DDoS (Distributed Denial of Service),
2. dostawie wraz z wdrożeniem systemu bezpieczeństwa Anti-Bot,
3. wdrożeniu posiadanej przez Zamawiającego wersji R77 CheckPoint (Zamawiający ma prawo aktualizacji do grudnia 2014 r.),
4. reorganizacji posiadanego przez Zamawiającego systemu TippingPoint monitorującego zagrożenia bezpieczeństwa w sieci. Reorganizacja będzie polegała na wykonaniu relokacji segmentów objętych usługą IPS na bazie wytycznych zawartych w analizie systemu bezpieczeństwa,
5. opracowaniu scenariuszy testowych potwierdzających zgodność dostarczonych rozwiązań z SIWZ, zatwierdzeniu scenariuszy przez Zamawiającego i przeprowadzeniu testów zgodnie ze scenariuszami,
6. opracowaniu i przedstawieniu raportu z testów,
7. wykonaniu dokumentacji powykonawczej,
8. przeprowadzeniu szkoleń i warsztatów,
9. objęciu rozbudowanego Systemu bezpieczeństwa gwarancją.

Opis systemu posiadanego przez Zamawiającego.

Zamawiający posiada centralny system bezpieczeństwa zakupiony na podstawie umowy nr 75/SPIS/PN/ 2011 objęty gwarancją do 13.12.2014, składający się z dwóch współdziałających podsystemów:

1. System wykrywania włamań HP IPS seria N składa się z następujących typów urządzeń:
   1) dwa urządzenia IPS służące do bezpośredniej ochrony segmentów sieci,
   2) HP Security Management System służący do zarządzania urządzeniami IPS.

Dodatkowo urządzenia IPS są wyposażone w zewnętrzne urządzenia ZPHA zapewniające kontynuację transmisji w przypadku awarii urządzenia IPS.

Dane techniczne:

1) zestaw IPS1 składający się z urządzeń firmy HP Tipping Point S2500N ZPHA CU, ZPHA FO,
2) zestaw IPS2 składający się z urządzeń firmy HP Tipping Point S2500N ZPHA CU, ZPHA FO oraz urządzenie HP Security Management System HP SMS.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

2. System bezpieczeństwa w oparciu o rozwiązania firmy CheckPoint.

Platforma sprzętowa zbudowana została w oparciu o dwa serwery sprzętowe o następujących parametrach:

1) model x3650 M3,
2) zamontowane 2 procesory sześciordzeniowe (w sumie 12 rdzeni procesora (core CPU)),
3) zainstalowane 8 GB RAM,
4) zainstalowane 2 dyski twarde HDD 70 GB SAS (RAID 1),
5) napęd DVD,
6) zainstalowane 18 interfejsów RJ45, Ethernet 10/100/1000.

Dodatkowo na potrzeby zarządzania środowiskiem zainstalowany został serwer sprzętowy o następujących parametrach:

1) model x3650 M3,
2) zamontowane 2 procesory sześciordzeniowe (w sumie 12 rdzeni procesora (core CPU)),
3) zainstalowane 16 GB RAM,
4) zainstalowane 2 dysk twardy HDD 300 GB SAS,
5) napęd DVD,
6) zainstalowane 6 interfejsów RJ45, Ethernet 10/100/1000.

Serwery te stanowią parę redundantną urządzeń bezpieczeństwa – CheckPoint Cluster.

Stacja zarządzająca: HP Z600 2xXEON E5620 2.40 12MB/1066.

Na obu elementach klastra zostały zainstalowane systemy CheckPoint Secure Platform w wersji R75.20.
Zamawiający planuje zwiększenie przepustowości łącza do Internetu do 2*150Mbit/s, dlatego wszystkie oferowane produkty powinny zapewniać taką wydajność.

Szczegółowe informacje na temat posiadanych produktów firmy CheckPoint znajdują się na koncie 0005911325 w UserCenter CheckPoint, którego właścicielem jest Główny Urząd Statystyczny.

Wykonanie przedmiotu zamówienia obejmuje następujące zadania:

I. Dostawa i wdrożenie systemu bezpieczeństwa sieciowego DDoS (Distributed Denial of Service).

Zamawiający wymaga dostarczenia, instalacji i konfiguracji dwóch takich samych urządzeń DDoS (Distributed Denial-of-Service) o wyspecyfikowanej poniżej charakterystyce.

1. Urządzenie ma spełniać następujące wymagania:

   1) Tryb pracy:

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

a) urządzenie pracujące w trybie przezroczystym w trzeciej i drugiej warstwie sieciowej - nie wymaga modyfikacji w adresacji IP, nie wymaga modyfikacji routingu TCP/IP, nie wymaga adresowania na poziomie adresów Ethernet/MAC, może być włączone w dowolnym segmencie i przełączane między segmentami bez ograniczeń,

b) urządzenie może pracować jako sensor podłączony do portu monitorującego (tzw. port typu mirror).

2) Wydajność urządzenia: minimum 400 Mb/s ruchu oczyszczonego z ataków DoS i DDoS.

3) Liczba obsługiwanych segmentów sieci: minimum 2 segmenty sieci gigabitowej (10/100/1000 Gb/s).

4) Obsługa segmentów sieci w trybie fail-open (uszkodzone, niedziałające lub wyłączone urządzenie nie blokuje ruchu sieciowego).

5) Możliwości rozbudowy:

a) możliwość ochrony ruchu w dodatkowym (trzecim) segmencie sieci gigabitowej z połączeniami kablowymi lub światłowodowymi,

b) możliwość rozbudowy do klastra o podwyższonej niezawodności (tzw. tryb HA - High Availability).

6) Konfiguracja i zarządzanie urządzeniem:

a) urządzenie umożliwia szybką konfigurację podstawowych parametrów pracy przez dyżurującego operatora (funkcja opisywana jako tzw. Configuration Wizard - uproszczony tryb konfiguracji przez osobę nieprzeszkoloną),

b) zarządzanie przez port konsoli szeregowej (tzw. zarządzanie out-of-band),

c) zarządzanie sieciowe:
- linia poleceń, ruch szyfrowany,
- za pomocą przeglądarki, ruch zaszyfrowany,
- protokół SNMP (wersje 1, 2 i 3),
- protokół SYSLOG.

7) Urządzenie musi być wyposażone w podwójny system zasilania.

2. Wymagania dotyczące zakresu oferowanej ochrony DDoS:

1) System powinien zapewniać skuteczną ochronę przed atakami DoS/DDoS zorganizowaną w sposób modularny, umożliwiający elastyczność w doborze sposobów ochrony przed zagrożeniami.

2) System ma posiadać wielowarstwowe, działające niezależnie zabezpieczenia gwarantujące:

a) analizę statystyczną ruchu sieciowego TCP/IP, modelowanie i automatyczne filtrowanie anomalii sieciowych (ochrona przed atakami typu Network Flood),

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

b) analizę statystyczną ruchu DNS, modelowanie i automatyczne filtrowanie anomalii aplikacyjnych związanych z ruchem DNS (ochrona przed atakami typu DNS Flood),
c) analizę statystyczną ruchu HTTP, modelowanie i automatyczne filtrowanie anomalii aplikacyjnych związanych z ruchem HTTP (ochrona przed atakami typu HTTP Page Flood),
d) automatyczne wykrywanie serwerów WWW i tworzenie dla wykrytych serwerów profilu ochronnego,
e) wykrywanie ataków na podstawie sygnatur narzędzi generacji pakietów,
f) wykrywanie anomalii w pakietach TCP/IP,
g) wykrywanie anomalii w sesjach TCP/IP,
h) generację filtrów: poniżej 30 sekund od ataku,
i) precyzję filtrowania: automatyczne zwiększanie dokładności filtrowania.

3) System ma zapewnić korelację zdarzeń, dokumentację oraz wizualizację informacji o atakach:

a) klasyfikacja ataków i prezentacja wyników w podziale na:
- typy ataków: wolumetryczne typu flood, ataki typu slow-and-low, ataki sieciowe, aplikacyjne itd),
- poziomy zagrożenia (krytyczne, groźne, niegroźne),
- czas ataku (początek, koniec),
- geograficzne rozłożenie źródeł ataku (kraje pochodzenia).

b) śledzenie informacji o liczbach pakietów, transmitowanym ruchu, adresach IP zaangażowanych w atak,

c) kopiowanie pakietów atakujących do kolektorów pakietów w celu dokumentacji zdarzenia i gromadzenia dowodów (funkcja packet trace na poziomie sieciowym).

3. Wymagania dotyczące współpracy z systemami zarządzania bezpieczeństwem CheckPoint Zamawiającego:

Urządzenie powinno współpracować z systemem zarządzania CheckPoint Security Management System posiadanym przez Zamawiającego w zakresie bezpośredniej współpracy z modułami minimum: CheckPoint SmartView Tacker, CheckPoint SmartEvent. Zamawiający nie ogranicza rozwiązań technicznych do właściwych dla producenta posiadanego systemu.

II. Dostawa wraz z wdrożeniem systemu bezpieczeństwa Anti-Bot,

Anti-Bot jest to funkcjonalność odpowiedzialna za wykrywanie aktywności sieciowej botów (malware), blokowanie ich komunikacji oraz ostrzeżenie administratora o niebezpieczeństwie w jego sieci pod postacią zainfekowanego komputera.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

Podstawowe funkcjonalności systemu:

1. Kontrola całego ruchu sieciowego wychodzącego z firmy na poziomie bramy internetowej.
2. Wykrywanie zainfekowanych złośliwym oprogramowaniem typu bot oraz atakami APT komputerów w sieci firmowej, przeciwdziałając generowaniu spamu, rozsyłaniu malware.
3. Ostrzeganie administratora o niebezpieczeństwie w sieci firmy pod postacią zainfekowanego komputera.
4. Analiza wzorców ruchu sieciowego w chronionych środowiskach.
5. Aktualizacje praktycznie w czasie rzeczywistym.
6. Blokowanie niebezpiecznej komunikacji do centrów zarządzania sieciami Botnet.
7. Korelacja informacji pochodzących z wielu źródeł, takich jak:
   - Listy adresów IP, adresów URL, domen oraz serwerów DNS wykorzystywanych do popełniania przestępstw internetowych,
   - Sposoby komunikacji malware w sieciach Botnet.

Podstawowe cechy systemu:

1. Umiejętność poszukiwania zainfekowanych komputerów przy pomocy informacji przesyłanych przez bramę internetową.
2. Wyrywanie urządzeń zaatakowanych złośliwym oprogramowaniem typu bot.
3. Niezależność od zainstalowanego na komputerach oprogramowania.
4. Analiza ruchu sieciowego pod kątem łączności z zewnętrznymi ośrodkami sterowania i blokowanie takich transmisji.
5. Funkcja raportowania komputerów pracujących pod zewnętrzną kontrolą.

Współpraca modułu z systemem zarządzania CheckPoint Security Managament System posiadanym przez Zamawiającego w zakresie bezpośredniej współpracy z modułami: CheckPoint Smart View Tracker, CheckPoint Smart Event Zamawiający nie ogranicza rozwiązań technicznych do właściwych dla producenta posiadanego systemu.

III. Aktualizacja oraz rozbudowa o nowe elementy posiadanego przez Zamawiającego systemu CheckPoint polega na:

1. aktualizacji systemu CheckPoint (2 x Gateway + Management) z wersji R75.20 do posiadanej przez Zamawiającego wersji R77 wraz z kompletną wymianą podsystemu dyskowego w serwerze zarządzania Management (zwiększenie pojemności systemu dyskowego – dwa dyski posiadane przez Zamawiającego),

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

2. przebudowie polityki bezpieczeństwa związanej z instalacją systemu DDoS, migracją systemu CheckPoint do posiadanej przez Zamawiającego wersji R77 i wytycznymi z analizy systemu bezpieczeństwa oraz aktywacją i konfiguracją nowego elementu systemu Anti-Bot,
3. reorganizacji sytemu TippingPoint, obejmującej projekt i wykonanie relokacji segmentów objętych usługą IPS na bazie wytycznych zawartych w analizie systemu bezpieczeństwa.

IV. Wykonanie dokumentacji powykonawczej zawiera:

1. opis zainstalowanego oprogramowania z informacjami o sposobie konfiguracji,
2. procedury administracyjne w zakresie posiadanych przez Zamawiającego oraz wdrażanych systemów:
   1) konfiguracja sprzętowa wszystkich elementów systemu bezpieczeństwa,
   2) ustawienia konfiguracyjne systemu posiadanej przez Zamawiającego wersji CheckPoint R77,
   3) ustawienia konfiguracyjne serwera IBM x3650,
   4) procedury konfiguracji ustawień kontrolera RAID,
   5) procedury migracji z obecnego rozwiązania do nowej architektury,
   6) procedura instalacji systemu posiadanej przez Zamawiającego wersji CheckPoint R77,
   7) procedura instalacji systemu CheckPoint SMS dla posiadanej wersji R77,
   8) procedura backup oraz snapshot.
   9) testy akceptacyjne potwierdzające zgodność wykonanych prac z SIWZ.

V. Szkolenia i warsztaty

Wykonawca przeprowadzi cykl szkoleń dla pracowników Zamawiającego.

A. Szkolenie obejmujące posiadany przez Zamawiającego system CheckPoint R77 przeprowadzone zgodnie z następującymi wymaganiami:

   1) ilość uczestników – 2 osoby,
   2) czas trwania szkolenia: 5 dni roboczych (40 godzin),
   3) szkolenie zostanie przeprowadzone na środowisku testowym poza siedzibą Zamawiającego,
   4) program szkolenia musi zawierać całość zagadnień obejmujących instalacje, konfiguracje, administrowanie systemem oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie,
   5) wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej i elektronicznej w formacie PDF,
   6) wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia.

B. Szkolenie obejmujące system DDoS przeprowadzone zgodnie z następującymi wymaganiami:
   1) ilość uczestników – 2 osoby,

2) czas trwania szkolenia: 2 dni robocze (24 godzin),
3) szkolenie zostanie przeprowadzone na środowisku testowym poza siedzibą Zamawiającego,
4) program szkolenia musi zawierać całość zagadnień obejmujących instalacje, konfiguracje, administrowanie systemem oraz zapewnić umiejętności i wiedzę niezbędną w tym zakresie,
5) wszyscy uczestnicy szkolenia muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej i elektronicznej w formacie PDF,
6) wszyscy uczestnicy szkolenia otrzymają zaświadczenia potwierdzające ukończenie szkolenia.

C. Warsztaty obejmujące system DDoS przeprowadzone zgodnie z następującymi wymaganiami:

1) ilość uczestników – 2 osoby,
2) czas trwania warsztatu: 2 dni robocze,
3) warsztaty zostaną przeprowadzone na środowisku produkcyjnym Zamawiającego w siedzibie Zamawiającego.
4) program warsztatów musi obejmować:
   a) analizę problemów związanych z platformą bezpieczeństwa (incydenty bezpieczeństwa, wykryte nowe zagrożenia np. na bazie analizy logów systemowych) i pomoc w ich neutralizacji na bazie posiadanego przez Zamawiającego sprzętu i oprogramowania,
   b) ocenę wpływu na politykę bezpieczeństwa i pomoc w implementacji nowych elementów konfiguracji systemów bezpieczeństwa.
5) wszyscy uczestnicy warsztatów muszą otrzymać materiały szkoleniowe w języku polskim lub angielskim, w formie papierowej lub elektronicznej w formacie PDF.

D. Wykonawca pokryje wszelkie koszty związane z dojazdem pobytem oraz wyżywieniem i zakwaterowaniem wykładowców, którzy będą prowadzili szkolenie.

E. Wykonawca pokryje wszelkie koszty związane z pobytem oraz wyżywieniem i zakwaterowaniem uczestników.

F. Wykonawca zapewni każdemu uczestnikowi szkolenia oraz warsztatów samodzielne stanowisko pracy, napoje w czasie przerw oraz posiłek (obiad).

G. Na co najmniej 14 dni przed rozpoczęciem szkoleń Wykonawca przedstawi Zamawiającemu do akceptacji – harmonogram szkoleń przygotowany w porozumieniu z Zamawiającym obejmujący:

1) programy szkoleń zawierające szczegółowe informacje o zakresie tematycznym i rozkładzie zajęć dla poszczególnych szkoleń,

2) metodę i formę prowadzenia szkoleń,

3) listę wykładowców i informacje o wykładowcach którzy przeprowadzą poszczególne szkolenia.

H. Wykonawca zobowiązany będzie do przeprowadzenia szkoleń/warsztatów zgodnie z zatwierdzonym przez zamawiającego szczegółowym zakresem tematycznym i harmonogramem szkoleń.

I. Potwierdzeniem prawidłowo przeprowadzonego szkolenia/warsztatu jest pozytywna ocena minimum 4 w arkuszu indywidualnej oceny szkolenia (wzór Arkusza AIOS – załącznik nr 5 do umowy).

J. Wykonawca w ramach prowadzonych szkoleń oraz warsztatów zobowiązany jest przekazać Zamawiającemu:

1) materiały szkoleniowe,

2) ankiety oceny szkoleń,

3) listy obecności.

K. Listę wydanych Zaświadczeń i komplet imiennych zaświadczeń dla wszystkich uczestników, którzy ukończą szkolenia, warsztaty pod warunkiem uczestnictwa w pełnym wymiarze zajęć.

VI. Warunki świadczenia gwarancji dla wdrożonego systemu.

Gwarancją mają być objęte produkty i oprogramowanie dostarczone przez Wykonawcę w ramach postępowania przetargowego oraz będące w posiadaniu Zamawiającego, które wejdą w skład rozbudowanego Systemu bezpieczeństwa:

- rozbudowany system Firewall: 3 lata
- IPS: 1 rok
- DDoS: 1 rok
- Anti-Bot 3 lata

1. Gwarancja realizowana będzie w siedzibie Zamawiającego.

Dopuszcza się kontakt mailowy i telefoniczny, pod warunkiem, że nie wpływa ona na obniżenie jakości świadczenia usług.

2. Świadczenie usług gwarancyjnych odbywać się będzie w dni robocze od poniedziałku do piątku, w godzinach od 8:00 do 17:00 lub wyznaczonych oknach serwisowych w ustalanych wcześniej godzinach.

3. Zamawiający nie będzie ponosił żadnych kosztów związanych z pełnieniem gwarancji przez wykonawcę (kosztów dojazdu, kosztów noclegu itp.).

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji

4. Wykonawca gwarantuje maksymalny czas reakcji na zgłaszane problemy nie dłuższy niż 24 godziny.

5. W tym okresie w ramach gwarancji Wykonawca zapewni: Cykliczne (minimum dwa razy w roku) przeglądy systemów bezpieczeństwa będących przedmiotem postepowania w siedzibie Zamawiającego zakończone raportem dotyczącym wykrytych problemów i nieprawidłowości oraz wskazaniem sposobu ich rozwiązania.

6. W okresie gwarancji Wykonawca musi zapewnić dostęp do bazy wiedzy, aktualnej wersji, aktualnych sygnatur oraz krytycznych poprawek producentów komponentów związanych z bezpieczeństwem i stabilnością działania Systemu w całym czasie trwania gwarancji.

7. Pomoc techniczną inżyniera Wykonawcy w sytuacji zagrażającej stabilnej pracy systemu bezpieczeństwa.

8. Pomoc techniczną inżyniera Wykonawcy w czasie wykonywania przez CIS planowanych instalacji poprawek, uaktualnień lub nowych wersji oprogramowania.

9. Pomoc techniczną inżyniera Wykonawcy, w tym zdalną diagnozę, w przypadku wystąpienia nieprzewidzianych problemów z oprogramowaniem.

10. Świadczenie konsultacji w zakresie eksploatacji, konfiguracji oraz funkcjonalności oprogramowania.

11. Wady Systemu objęte gwarancją klasyfikowane są jako: awarie, błędy i usterki:

    1) awaria (błąd krytyczny) oznacza niezgodne z dokumentacją, nieprawidłowe działanie Systemu, powodujące unieruchomienie całego Systemu lub znacznej jego części i brak dostępu do funkcji,

    2) błąd oznacza niezgodne z dokumentacją oraz powtarzalne nieprawidłowe działanie Systemu powodujące brak dostępu do funkcji używanych nie rzadziej niż raz w tygodniu przez większą liczbę użytkowników albo brak dostępu do ważnych funkcji Systemu,

    3) usterka oznacza niezgodne z dokumentacją działanie modułów systemu o mniejszym znaczeniu dla funkcjonalności Systemu.

12. Czas reakcji Wykonawcy od momentu przyjęcia zgłoszenia w ramach gwarancji do podjęcia działań naprawczych wynosi maksymalnie:
    1) dla awarii - 4 godziny,
    2) dla błędów - 12 godzin,
    3) dla usterki - 2 dni.

13. Wady Systemu objęte gwarancją mogą być zgłaszane wyłącznie przez osoby upoważnione ze strony Zamawiającego, drogą pisemną - pocztą elektroniczną, faksem lub telefonicznie.

14. Usunięcie wady Systemu polega na przywróceniu pełnej poprawności działania Systemu. Usunięcie wady w okresie trwania gwarancji następuje na wyłączny koszt i ryzyko Wykonawcy. Wszystkie koszty związane z usunięciem wady w szczególności koszty gwarancji, transportu i naprawy obciążają Wykonawcę.
15. Czas na usunięcie zgłoszonych wad systemu od chwili podjęcia działań naprawczych wynosi maksymalnie:
    1) dla awarii - 48 godzin,
    2) dla błędów - 3 dni,
    3) dla usterki - 7 dni.
16. W przypadku niewykonania naprawy gwarancyjnej w miejscu i w terminie, o którym mowa powyżej, Wykonawca zobowiązuje się dostarczyć na czas naprawy takie samo urządzenie wolne od wad i zapewni jego prawidłowe działanie. Ostateczny termin usunięcia usterki uszkodzonego urządzenia nie może być dłuższy niż 30 dni od dnia zgłoszenia jego wady lub usterki.
17. Wykonawca zobowiązuje się do wymiany urządzenia na nowe w przypadku, gdy po wykonaniu dwóch napraw gwarancyjnych dostarczonego urządzenia będzie ono wykazywało nadal wady w działaniu.
18. W przypadku nie wywiązania się Wykonawcy ze swoich zobowiązań (patrz punkt 5) Zamawiający może dokonać tych czynności we własnym zakresie i kosztami obciążyć Wykonawcę.
19. Wykonawca pokrywa wszelkie koszty związane z naprawami gwarancyjnymi.
20. Zamawiający zobowiązany jest do udzielenia szczegółowych informacji o zewnętrznych objawach wady lub usterki oraz czasie jej wystąpienia.
21. W przypadku naprawy gwarancja ulega przedłużeniu o czas naprawy.
22. Zamawiający ma prawo dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, a także prawo do przemieszczenia zainstalowanego sprzętu bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne przedmiotu Umowy powstałe z winy pracowników Zamawiającego.

BENEFICJENT:
GŁÓWNY URZĄD STATYSTYCZNY
al. Niepodległości 208
00-925 Warszawa

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz ze środków budżetu państwa.
7. Oś Priorytetowa: Społeczeństwo informacyjne – budowa elektronicznej administracji