Załącznik Nr 1 do SIWZ

I. Opis założeń projektu:

„Konto przedsiębiorcy – usługi online dla firm w jednym miejscu”

Ministerstwo Przedsiębiorczości i Technologii realizuje projekt pn. „Konto przedsiębiorcy – usługi online dla firm w jednym miejscu”. Projekt jest realizowany w ramach Programu Operacyjnego Polska Cyfrowa, działanie 2.1 „Wysoka dostępność i jakość e-usług publicznych”, współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego. Celem projektu jest usprawnienie zakładania i prowadzenia działalności gospodarczej w Polsce poprzez Punkt Informacji dla Przedsiębiorcy wraz z Kontem firmy, na którym będą przechowywane i prezentowane dane potrzebne do realizacji usług. Udostępnienie planowanych e-usług oraz konsolidacja serwisów będą centralnym miejscem dla przedsiębiorców chcących załatwiać sprawy firmowe przez Internet. Konto Firmy umożliwi także załatwianie spraw przez pełnomocników i reprezentantów firm oraz aktualizację danych w CEIDG. Serwis Biznes.gov.pl umożliwi przedsiębiorcom i ich pełnomocnikom kontakt z Rzecznikiem MŚP oraz tworzenie zapytań w kontekście konkretnych opisów usług lub objaśnień prawnych.

II. Opis przedmiotu zamówienia

Przedmiotem zamówienia jest wykonanie audytu bezpieczeństwa dwóch systemów informatycznych:

1. Centralnej Ewidencji i Informacji o Działalności Gospodarczej (zwanej dalej także CEIDG),

2. Punktu Informacji dla Przedsiębiorcy (zwanego dalej także serwisem biznes.gov.pl),

oraz audytu wydajności Punktu Informacji dla Przedsiębiorcy. Celem głównym audytów jest określenie poziomu bezpieczeństwa systemów, wskazanie punktów obniżających ten poziom oraz zaproponowanie rozwiązań, które doprowadzą do uzyskania akceptowalnego przez Zamawiającego poziomu bezpieczeństwa. Audyt wydajności ma na celu identyfikację podatności i nieprawidłowości, które mogą stanowić zagrożenie dla stabilności i ciągłości działania systemu.

W ramach przedmiotowych audytów, wykonawca powinien przeprowadzić trzy procesy audytowe obejmujące audyt bezpieczeństwa oraz trzy procesy audytowe wydajności.

W ramach audytów przewiduje się obecność i zaangażowanie przedstawicieli Wykonawcy w miejscu wykonywania zamówienia. Wykonawca wskaże osobę lub osoby o profilu inżyniera bezpieczeństwa IT, które będą wykonywały zadania doradcze i kontrolne, uzgodnione z Zamawiającym. Przewidywany wymiar zaangażowania w wykonanie części zadań audytorskich na miejscu wynosi 85 osobodni.

Do zadań Wykonawcy świadczącego usługi inżyniera bezpieczeństwa przy realizacji projektu „Konto przedsiębiorcy – usługi online dla firm w jednym miejscu” będzie należało m.in:

- Doradztwo w zakresie wdrożeń rozwiązań informatycznych obszaru monitorowania bezpieczeństwa IT;

- Analiza zagrożeń zewnętrznych i wewnętrznych obszaru cyberbezpieczeństwa;

- Detekcja błędów aplikacyjnych;

- Recenzja architektury logicznej;

- Analiza podatności występujących w zainstalowanej wersji serwera;

- Skanowanie podatności w udostępnionych usługach sieciowych;

- Detekcja podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji);

- Próba eskalacji ataku na pozostałe maszyny, systemy w LAN po przejęciu kontroli nad jedną z aplikacji;

- Analiza kodu źródłowego aplikacji.

III. Szczegółowy Opis Przedmiotu Zamówienia dla audytu bezpieczeństwa Punktu Informacji dla Przedsiębiorcy

Przedmiotem umowy jest wykonanie trzech edycji audytu bezpieczeństwa konfiguracji urządzeń sieciowych i aplikacji webowych systemu elektronicznego Punktu Informacyjnego dla Przedsiębiorcy w szczególności:

1. **Audyt infrastruktury** Punktu Informacji dla Przedsiębiorcy, w zakresie:

a) analizy wersji oprogramowania pod kątem znanych podatności,

b) analizy konfiguracji dostępu do urządzeń,

c) przeglądu konfiguracji dot. użytkowników korzystających z urządzeń, prawa dostępu, listy dostępów, testy słabych haseł,

d) analizy konfiguracji i reguł VPN,

e) analizy wykorzystanych mechanizmów kryptograficznych,

f) analizy zasad filtracji ruchu sieciowego,

g) analizy pod kątem obecności niepożądanych usług,

h) analizy mechanizmów logowania zdarzeń.

Tabela 1. Lista urządzeń Punktu Informacji dla Przedsiębiorcy

1.	klaster Juniper SRX 650
2.	Juniper SRX550
3.	Fortinet Fortiweb 1000D
4.	Przełącznik sieciowy Cisco Catalyst 2960-X

2. **Audyt aplikacji webowych** - *.biznes.gov.pl, w tym pentesty portalu WWW, w zakresie:
   a) walidacja danych wejściowych w tym:
      - pliki cookie,
      - nagłówki.
   b) Parametry wysyłane metodami http:
      - badanie sesji użytkowników aplikacji,
      - badanie komunikatów błędów,
      - badanie mechanizmów przekierowań,
      - badanie danych zapisywanych do bazy danych,
      - badanie integralności logów aplikacji,
      - szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS),
      - badanie błędów logicznych aplikacji w miejscach krytycznych.
   c) Badanie środowiska pracy aplikacji:
      - uprawnień w systemie do plików oraz zasobów,
      - użytego oprogramowania podnoszącego poziom bezpieczeństwa,
      - architektury systemu dotyczącej wszelkich obszarów bezpieczeństwa (składowanie logów, obsługa wyjątków itd.),
      - konfiguracji serwerów, z których korzysta aplikacja pod kątem bezpieczeństwa.
3. **Audyt konfiguracji systemów operacyjnych i baz danych środowiska produkcyjnego,** w zakresie:
   a) analizy architektury i technologii platformy,
   b) analizy konfiguracji serwerów (+uprawnień plików/katalogów),

c) analizy architektury i technologii bazy danych,

d) analizy konfiguracji aplikacji bazy danych,

e) analizy dostępu do bazy danych i uprawnień,

f) analizy mechanizmów logowania,

g) analizy możliwych ataków

4. **Celem audytu jest:**

a) wykonanie prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa ST Punktu Informacji dla Przedsiębiorcy,

b) dostarczenie wniosków, zaleceń, rekomendacji w celu dokładnego rozpoznania i redukcji wskazanych podatności oraz wskazanie adekwatnych działań mających na celu wyeliminowanie zagrożeń.

5. **Przeprowadzone badania i analiza w trakcie audytu powinny wskazać podatności i zagrożenia wynikające z:**

a) zastosowanych technologii i standardów zabezpieczeń,

b) słabości oprogramowania oraz poprawności konfiguracji systemów sieciowych,

c) faktu istnienia styków sieci o różnym charakterze, np. styku z siecią Internet, styku systemów z innymi sieciami, w tym potencjalne zagrożenia ze strony sieci zewnętrznej,

d) polityk bezpieczeństwa skonfigurowanych na ww. urządzeniach.

6. **Wynikiem każdego procesu audytu ma być raport,** opisujący poszczególne działania i testy które zostały wykonane, obejmujący wykryte podatności i wynikające z nich zagrożenia, w tym sporządzenie listy ewentualnych nieprawidłowości oraz sformułowanie zaleceń, które przyczynią się do zwiększenia bezpieczeństwa systemu, zawierający minimum:

a) streszczenie dla kierownictwa,

b) opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mają□ymi □□ □□lu □mi□im□li□ow□□i□ bądź □□łkowitą r□duk□ję ryzyka związanego z wykrytymi podatnościami,

c) propozycje uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających o□hro□□ę przed możliwymi atakami sieciowymi i aplikacyjnymi,

d) opis ryzyk dla systemu informatycznego,

e) rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa.

Proces audytowy zostanie wykonany w trzech iteracjach (procesach audytowych).. Pierwszy proces

audytowy obejmować będzie pełny zakres prac opisanych w sekcji III niniejszego dokumentu. Drugi proces audytowy obejmować będzie dodatkowo weryfikację usunięcia podatności i implementacji poprawek wykazanych w I procesie. Trzeci proces audytowy obejmować będzie wykonanie prac opisanych w sekcji III niniejszego dokumentu w zakresie zmian i nowych usług oraz funkcjonalności udostępnionych w systemie, jak również weryfikację usunięcia podatności i implementacji poprawek wykazanych w drugim procesie audytowym.

Precyzyjny zakres konkretnej iteracji zostanie wskazany w zleceniu wystawionym przez Zamawiającego przed rozpoczęciem procesu.

IV. Szczegółowy Opis Przedmiotu Zamówienia audytu bezpieczeństwa CEIDG.

Przedmiotem umowy jest wykonanie audytu bezpieczeństwa konfiguracji urządzeń sieciowych i aplikacji webowej systemu **Centralnej Ewidencji i Informacji o Działalności Gospodarczej** (CEIDG) w szczególności:

7. **Audyt infrastruktury CEIDG,** w zakresie:
   a) analiza wersji oprogramowania pod kątem znanych podatności,
   b) analiza konfiguracji dostępu do urządzenia,
   c) przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
   d) analiza konfiguracji i reguł VPN,
   e) analiza wykorzystanych mechanizmów kryptograficznych,
   f) analiza zasad filtracji ruchu sieciowego,
   g) analiza pod kątem obecności niepożądanych usług,
   h) analiza mechanizmów logowania zdarzeń.

Tabela 1. Lista urządzeń CEIDG.

1.	Juniper SRX 650
2.	Juniper J6350
3.	Fortinet Fortiweb 1000C
4.	Przełącznik sieciowy Cisco SG 200-18

2. **Audyt aplikacji webowej** - ceidg.gov.pl, w tym pentesty portalu WWW, w zakresie:

d) walidacja danych wejściowych w tym:
   - pliki cookie,
   - nagłówki.

e) Parametry wysyłane metodami http:
   - badanie sesji użytkowników aplikacji,
   - badanie komunikatów błędów,
   - badanie mechanizmów przekierowań,
   - badanie danych zapisywanych do bazy danych,
   - badanie integralności logów aplikacji,
   - szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS),
   - badanie błędów logicznych aplikacji w miejscach krytycznych.

f) Badanie środowiska pracy aplikacji:
   - uprawnień w systemie plików oraz zasobów,
   - wersji usług,
   - użytego oprogramowania podnoszącego poziom bezpieczeństwa,
   - architektury systemu dotyczącej wszelkich obszarów bezpieczeństwa (składowanie logów, obsługa wyjątków itd.),
   - konfiguracji serwerów, z których korzysta aplikacja pod kątem bezpieczeństwa.

3. **Audyt konfiguracji systemów operacyjnych i baz danych środowiska produkcyjnego,** w zakresie:

a) analizę architektury i technologii platformy,

b) analizę konfiguracji serwera (+uprawnień plików/katalogów),

c) analizę architektury i technologii bazy danych,

d) analizę konfiguracji aplikacji bazy danych,

e) analizę dostępu do bazy danych, uprawnień,

f) analizę mechanizmów logowania,

g) analizy możliwych ataków.

4. **Celem audytu jest:**

c) wykonanie prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa ST CEIDG,

d) dostarczenie wniosków, zaleceń, rekomendacji w celu dokładnego rozpoznania i redukcji wskazanych podatności oraz wskazanie adekwatnych działań mających na celu wyeliminowanie zagrożeń.

5. **Przeprowadzone badania i analiza w trakcie audytu powinny wskazać podatności i zagrożenia wynikające z:**

   e) zastosowanych technologii i standardów zabezpieczeń,

   f) słabości oprogramowania oraz poprawności konfiguracji systemów sieciowych,

   g) faktu istnienia styków sieci o różnym charakterze, np. styku z siecią Internet, styku systemów z innymi sieciami, w tym potencjalne zagrożenia ze strony sieci zewnętrznej,

   h) polityk bezpieczeństwa skonfigurowanych na ww. urządzeniach.

6. **Wynikiem każdego procesu audytu ma być raport,** opisujący poszczególne działania i testy które zostały wykonane, obejmujący wykryte podatności i wynikające z nich zagrożenia, sporządzenie listy ewentualnych nieprawidłowości oraz sformułowanie zaleceń, które przyczynią się do zwiększenia bezpieczeństwa systemu zawierający minimum:

   a) streszczenie dla kierownictwa,

   b) opi□ □□□l□□io□y□h pod□t□oś□i w obu ob□□□r□□h wr□□ □ □□l□□□□i□mi i r□kom□□d□□j□mi m□ją□ymi □□ □□lu □mi□im□li□ow□□i□ bądź □□łkowitą r□duk□ję ryzyka związanego z wykrytymi podatnościami,

   c) propozycje uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających o□hro□□ę przed możliwymi atakami sieciowymi i aplikacyjnymi,

   d) opis ryzyk dla systemu informatycznego,

   e) rekomendacje w zakresie rozbudowy systemu informatycznego w zakresie podniesienia bezpieczeństwa.

Proces audytowy zostanie wykonany w trzech iteracjach (procesach audytowych).. Pierwszy proces audytowy obejmować będzie pełny zakres prac opisanych w sekcji III niniejszego dokumentu. Drugi proces audytowy obejmować będzie dodatkowo także weryfikację usunięcia podatności i implementacji poprawek wykazanych w I procesie. Trzeci proces audytowy obejmować będzie wykonanie prac opisanych w sekcji III niniejszego dokumentu w zakresie zmian i nowych usług oraz funkcjonalności udostępnionych w systemie, jak również weryfikację usunięcia podatności i implementacji poprawek wykazanych w drugim procesie audytowym.

Precyzyjny zakres konkretnej iteracji zostanie wskazany w zleceniu wystawionym przez Zamawiającego przed rozpoczęciem procesu.

V. Wymagania dotyczące audytu wydajności Punktu Informacji dla Przedsiębiorcy

1. Wprowadzenie:

Punkt Informacji dla Przedsiębiorcy składa się z następujących autonomicznych acz współpracujących elementów:

a) System Konfiguratora ElF
b) System Runtime ElF
c) Aplikacja Zaplecza
d) API Zaplecza
e) Podsystem logowania/rejestracji
f) CMS dla treści portalowych

Celem przeprowadzenia audytu wydajności jest identyfikacja podatności i nieprawidłowości, które mogą stanowić zagrożenie dla stabilności i ciągłości działania systemu. Poza zapewnieniem kwestii ogólnie pojętej wydajności systemu, testy mają również wykryć potencjalne błędy które mogą przyczynić się do zaburzenia ciągłości i stabilności działania systemu oraz ewentualnie wskazać zalecane parametry dla konfiguracji systemu poprawiające jego wydajność. Wynikiem każdego procesu audytu ma być raport z testów i identyfikacja potencjalnych wąskich gardeł.

2. Testy:

Celem testów jest ustalenie :
- liczby sesji dla której charakterystyka obciążenia w funkcji czasu odchodzi od zależności liniowej (średni czas odpowiedzi ładowania strony zaczyna rosnąć gwałtownie),
- liczby sesji dla której czas średni odpowiedzi (ładowania strony) zaczyna rosnąć,
- liczba sesji dla której czas średni odpowiedzi (ładowania strony) wynosi maksymalnie 10 sek.

Do testów należy założyć, że średnio akcja użytkownika w sesji skutkująca przeładowanie strony odbywa się przeciętnie co 10 sekund.

Testy wydajności powinny uwzględniać:
- Upload załączników realizowanych metodą HTTP POST,
- Testy end-end z uwzględnieniem ograniczeń łącza dostępowego symetrycznego (dla 50, 100, 150, 200 Mb),
- Testy z pominięciem ograniczeń jakie wprowadza wydajność łącza dostępowego,

3. Zakres audytu:

a) **System Runtime eLF**

Testy serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów odpowiedzi serwera i czasu załadowania stron (liczona jako osiągnięcie stanu aplikacji JS na przeglądarce, objawiająca się odpowiednim HTML). Kolejne strony są sterowane i przełączane w ramach danej sesji przez aplikację JS (nie ma możliwości wywołania ich przechodząc do ich URL). Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.
Aplikacja działa w oparciu o AngularJS oraz mikroserwisy, co może wymagać od systemu testującego symulowanie rzeczywistych działań przeglądarki przez uruchomienie aplikacji JS.

Elementami pełnej sesji użytkownika jest podpisanie oraz przesłanie pliku, a na jej koniec upload utworzonego dokumentu (wielkość dokumentu 1MB, 5MB, 10MB). W trakcie samej sesji mogą być również przesyłane załączniki.

b) **System Konfigurator eLF i Aplikacja Zaplecza**

Testy serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów odpowiedzi serwera i czasu załadowania strony (gotowość usługi dla: nowa usługa, edycja usługi) Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.

Konfigurator eLF działa w oparciu o AngularJS oraz mikroserwisy, co może wymagać od systemu testującego symulowanie rzeczywistych działań przeglądarki przez uruchomienie aplikacji JS.
Aplikacja Zaplecza (PHP) wymaga dodatkowo symulacji logowania na jedno lub wiele indywidualnych kont.

c) Podsystem logowania/rejestracji

Test serwera www: dla jednoczesnych sesji: 0…5000 – pomiar czasów załadowania strony
Podsystem ten wymaga przeprowadzenia testów dwóch procesów.
Procesu rejestracji:
- wypełnienie i przesłanie formularza,
- odebranie wiadomości z kodem,
- wprowadzenie otrzymanego kodu w formularzu na stronie

Procesu logowania:
- zalogowanie się na utworzone konto,
- symulacje działań użytkownika w serwisie w szczególności:

d) API Zaplecza

- Średni i maksymalne czasy odpowiedzi dla dwu rodzajów zapytań:
- Zapytania proste (zawierające listę parametrów, zmieniających się przy wywołaniach w ramach zdefiniowanych zakresów lub random)
  - /ApiProcedures/getDetails
  - /ApiCommons/getPKD
  - /ApiInstitutions/getCategories
  - /ApiProcedures/getList
  - /ApiPublications/getDetails
  - /ApiCommons/getPKDDetails
  - /ApiProcedures/getThematicCategories
  - /ApiInstitutions/getDetails
  - /ApiGuide/getList
  - /ApiProcedures/getProfessionCategories
  - /ApiPnaAddress/getListByPostCode
  - /ApiPnaAddress/getStreetHints
- Zapytania złożone - sekwencja wywołań, która przyjmuje wartości otrzymane w odpowiedziach poprzedających zapytań:
  - /ApiGuide/getDescription
  - /ApiGuide/startGuide
  - /ApiGuide/setAnswer
    - ❖ wielokrotnie, aż odpowiedź wskaże, że to ostatnie pytanie
  - /ApiGuide/getSummary
  - /ApiGuide/getPDFGuide
- Każdy z testów dla 0…10 000 jednoczesnych zapytań

API nie wymaga logowania, jednak w samych zapytaniach złożonych ważna jest kolejność oraz przeparsowania odebranych odpowiedzi. Na początku sesji jest wymaganie odczytanie otrzymanego Hash w celu wykorzystania go do dalszej komunikacji.

e) Wysyłanie powiadomień e-mail

Ocenie podlega maksymalna przepustowość wysyłania e-maili przez API. Test powinien składać się z dwóch części:

- Test wydajności API przyjmującego e-maile do wysyłki i zapisujące je w buforze/kolejce
- Test wydajności rozwiązania wysyłającego emaile z bufora/kolejki.

System wymaga monitorowania zarówno ilości wywołań przesłanych do API oraz kolejki Mail Transfer Agent . Wiadomości muszą być przesyłane na istniejące konta na serwerze Mail Transfer Agent należącym do testującego w celu uniknięcia obniżenia reputacji domeny oraz adresacji testowanego systemu.

f) CMS

Testy serwera www dla jednoczesnych sesji: 0…5000 – pomiar czasów odpowiedzi serwera i czasu załadowania:

- Strony głównej
- Strony kategorii spraw
- Kilku przykładowych spisów spraw w kategorii
- Kilku przykładowych spisów treści w sprawie
- Kilku przykładowych ulotek z wybranej sprawy
- Kilku przykładowych stron statycznych

Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.

4. Produkty testów:

Końcowym produktem każdego z wykonanych testów powinien być raport prezentujący i zawierający:

- wyniki pomiarów badanych parametrów,
- ocenę tych wyników oraz ocenę ich wpływu na stabilność działania całego systemu,
- opis wykrytych zagrożeń wynikających z pomierzonych wartość badanych parametrów zawierający między innymi charakter zagrożenia, szczegółowy opis podatności oraz zalecenia umożliwiające ograniczenie lub wyeliminowanie podatności,

5. Wymagania dotyczące procesu testowania:

Każdy z trzech procesów audytowych przeprowadzony zostanie w następujących etapach:

- W pierwszym etapie Wykonawca przygotuje i przeprowadzi pierwszy test poszczególnych elementów zakresu audytu i przedstawi zamawiającemu raport z ich przeprowadzenia.
- W kolejnym etapie na podstawie analizy przedstawionych raportów Zamawiający zakłada dostrajanie konfiguracji poszczególnych elementów systemu i ponowne przeprowadzenie od 5 do ok. 20 iteracji takich dodatkowych testów w okresie maksymalnie do 3 miesięcy od czasu wykonania pierwszego testu. Zamawiający gwarantuje zlecenie wykonanie co najmniej 3

iteracji dodatkowych testów dla każdego z elementów zakresu audytu i maksymalnie 100 iteracji dodatkowych testów dla wszystkich elementów zakresu audytu łącznie.

Test powinien być przeprowadzony w metodologii mieszanej, która zakłada częściową znajomość testowanej architektury.

6. Specyfikacja architektury serwisu

- usługi Konfigurator ELF oraz Runtime ELF są uruchomione na środowisku typu PaaS – OpenShift Origin

- Aplikacja Zaplecza, API Zaplecza oraz Podsystem logowania/rejestracji są stworzone w języku PHP i korzystają z systemu baz danych MariaDB
- Aplikacja CMS jest stworzona w języku PHP i korzysta z systemu bazy danych PostgreSQL

- środowisko OpenShift znajduje się na kilku węzłach maszynach wirtualnych z systemem Linux – CentOS 7 (64-bity)

- Aplikacja Zaplecza, API Zaplecza oraz Podsystem logowania/rejestracji działają na jednym serwerze www (CentOS7/ Apache HTTPD 2.4), baza danych znajduje się na osobnej maszynie wirtualnej

- Aplikacja CMS działa na pojedynczym serwerze www (CentOS7 / Nginx 1.14), baza danych znajduje się na osobnej maszynie wirtualnej, serwer multimediów oraz plików statycznych znajduje się również na osobnej maszynie wirtualnej

- maszyny wirtualne Linux są uruchomione na kilku serwerach fizycznych w klastrze VMWare

- usługi są dostępne za pomocą protokołow HTTPS

- w przypadku aplikacji Zaplecze oraz Konto ruch na środowisku produkcyjnym jest puszczony przez system ochrony Exatel.

- usługi ELF a także konto są udostępnione przez proxy na serwerze portalu biznes.gov.pl w kontekstem URL – należy sprawdzić czy nie stanowi to wąskiego gardła systemu, na pewno jest to miejsce, gdzie awaria pojedynczego węzła może wpłynąć na dostępność całego systemu

- do logowania na usługi służy strona logowanie.biznes.gov.pl

- wszystkie dane znajduję się w serwerowni MPiT gdzie są wykonywane ich kopie zapasowe zarówno baz danych jak i całych maszyn wirtualnych

- w trakcie wykonywania kopii zapasowych w godzinach wieczornych i nocnych może wystąpić lekkie obniżenie wydajności systemu

VI. Harmonogram prac

1. W ramach przedmiotowych audytów Wykonawca przeprowadzi trzy procesy obejmujące audyt bezpieczeństwa systemów informatycznych Punkt Informacji dla Przedsiębiorcy i CEIDG:

a. pierwszy – rozpoczęcie i zakończenie orientacyjnie w I kwartale 2020 r.
b. drugi – rozpoczęcie i zakończenie orientacyjnie w III kwartale 2020 r.
c. trzeci – rozpoczęcie i zakończenie orientacyjnie w II kwartale 2021 r.

2. W ramach przedmiotowych audytów Wykonawca przeprowadzi trzy procesy obejmujące audyt wydajności Punktu Informacji dla Przedsiębiorcy (dwa etapy każdego z procesów):

a. pierwszy – rozpoczęcie i zakończenie orientacyjnie w I kwartale 2020 r.
b. drugi – rozpoczęcie i zakończenie orientacyjnie w III kwartale 2020 r.
c. trzeci – rozpoczęcie i zakończenie orientacyjnie w II kwartale 2021 r.

3. Wsparcie inżyniera bezpieczeństwa IT w miejscu wykonywania audyt przez cały czas trwania umowy, w łącznym wymiarze nie przekraczającym 85 osobodni. Przewidywane zapotrzebowanie na wsparcie w podziale na lata:

a. 2020 r. – 45 osobodni,

b. 2021 r. – 30 osobodni,

c. 2022 r. – 10 osobodni.

Wymienione zapotrzebowanie na wsparcie może ulec zmianie, w zależności od realizacji harmonogramu zadań projektowych.