Opis Przedmiotu Zamówienia

Cz. II – Audyt bezpieczeństwa i wydajności systemów teleinformatycznych MRiT – Biznes.gov.pl, CEIDG, Hurtownia Danych oraz wsparcie audytowe w zakresie pozostałych narzędzi utrzymywanych przez Ministerstwo

1. Przedmiot zamówienia

Przedmiotem zamówienia jest wykonanie audytów bezpieczeństwa i wydajności systemów teleinformatycznych wraz z usługą wsparcia eksperckiego inżyniera bezpieczeństwa IT zgodnie ze specyfikacją w poszczególnych rozdziałach.

Na przedmiot zamówienia składają się następujące zadania:

1. Wykonanie audytu bezpieczeństwa i wydajności systemu Biznes.gov.pl.

2. Wykonanie audytu bezpieczeństwa i wydajności systemów CEIDG i Hurtowni Danych.

3. Przeprowadzenie testów penetracyjnych oraz wydajności narzędzia do tworzenia ankiet i systemu CRM funkcjonujących w ramach projektu Innopoint.

4. Przeprowadzenie testów w zakresie bezpieczeństwa i wydajności przed wdrażaniem zmian lub nowych funkcjonalności w obrębie systemów Biznes.gov.pl, CEIDG i Hurtowni Danych – prawo opcji.

5. Realizacja doraźnych zleceń wsparcia w zakresie cyberbezpieczeństwa dot. systemów teleinformatycznych MRiT – prawo opcji.

Umowa zostanie zawarta na okres 24 miesięcy. Orientacyjny harmonogram zadań znajduje się w rozdz. V OPZ.

1. Opis systemów
2. Biznes.gov.pl

Biznes.gov.pl to serwis internetowy realizujący zadania Punktu Informacji dla Przedsiębiorcy (PIP), oraz Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), który udostępnia informacje oraz usługi e-administracji związane z rozpoczęciem, wykonywaniem (w tym uzyskiwaniem koncesji, zezwoleń, licencji) i kończeniem działalności gospodarczej w Polsce. Biznes.gov.pl ma dwie wersje językowe – polską oraz angielską. Treści każdej wersji dopasowane są do potrzeb użytkowników odpowiednio polsko- i angielskojęzycznych. Przygotowane narzędzie - serwis https://www.Biznes.gov.pl ma charakter intuicyjny i jest łatwy w użyciu.

Planowany dalszy kierunek rozwoju serwisu Biznes.gov.pl to optymalizacja zasobów portalu pod kątem potrzeb użytkowników oraz wymagań prawnych oraz rozwój części usługowej tak, aby portal stawał się usługowo-informacyjnym centrum informacji o zakładaniu i prowadzeniu działalności gospodarczej w Polsce dla przedsiębiorców polskich oraz zagranicznych.

Kluczowy kierunek dla dalszego rozwoju Systemu wynika bezpośrednio z realizacji przez Ministerstwo Rozwoju i Technologii projektu „Konto Przedsiębiorcy – usługi online dla firm w jednym miejscu”, w ramach którego dokonano połączenie CEIDG z serwisem Biznes.gov.pl oraz budową e-usług obejmujących możliwe działania na wpisie CEIDG, w tym rejestrację działalności gospodarczej w CEIDG.

W ramach powyższego podziału w portalu Biznes.gov.pl funkcjonują następujące treści:

- Opisy usług – usługą jest każda sprawa urzędowa, wynikająca z obowiązków nałożonych przez państwo i inicjowana przez obywatela. Opis usługi to przebieg postępowania administracyjnego, podatkowego lub sądowego. Ustandaryzowany opis usługi zawiera m.in. takie informacje jak: nazwę organu realizującego, opis kogo dotyczy procedura, wykaz potrzebnych dokumentów, termin załatwienia sprawy, wysokość należnej opłaty oraz sposób wnoszenia odwołań. Serwis obecnie udostępnia ok. 1,1 tys. opisów usług o zróżnicowanej objętości

- Artykuły – teksty publicystyczne dotyczące aktualnych zagadnień z zakresu tematyki interesującej dla przedsiębiorców m.in. wprowadzanych zmian w obszarze istotnym dla prowadzących działalności gospodarczą. Serwis obecnie udostępnia ok. 500 artykułów

- E-usługi – sprawy urzędowe, które są możliwe do zrealizowania elektronicznie, poprzez portal Biznes.gov.pl.

- FAQ - krótkie i precyzyjne odpowiedzi na najczęściej zadawane przez użytkowników portalu pytania. Odpowiedzi zawierają również przekierowania do treści portalu Biznes.gov.pl, które pogłębiają interesujący czytającego temat. Serwis obecnie udostępnia ok. 96 takich odpowiedzi

- Wzory dokumentów, np. wnioski, formularze do pobrania opracowane przez właściwy dla danej usługi organ. Stanowią uzupełnienie opisów usług oraz e-usług. Serwis obecnie udostępnia ok. 3,5 tys. wzorów dokumentów.

Tabela prezentuje systemy i aplikacje wchodzące w skład systemu (stan obecny na dzień publikacji ogłoszenia o zamówieniu):

|  |  |  |
| --- | --- | --- |
| Nazwa modułu | Opis | Wersje usług |
| Portal /serwis | Portal informacyjny dla obywateli autorskiego CMS’a. | Prod / test |
| eLF | Platforma usług elektronicznych służąca konfigurowaniu transakcyjnych publicznych usług online, ich testowaniu i ostatecznie produkcyjnemu udostępnianiu użytkownikom końcowym. Platforma składa się z dwóch podstawowych modułów: Konfigurator eLF i Runtime eLF | Prod / test |
| Zaplecze (Baza Wiedzy) | Moduł umożliwiający wyznaczonym pracownikom instytucji publicznych tworzenie i zarządzanie produktami w Bazie Wiedzy. | Prod / test |
| Akademia | Platforma e-learningowa dla użytkowników wraz z treściami multimedialnymi w postaci kursów i poradników | Prod / test |
| API (Baza Wiedzy) | Interfejs komunikacji do udostępnienia danych zgromadzonych w Bazie Wiedzy zarówno wewnętrznym modułom serwisu biznes,gov.pl (np. portal, platforma e-usług) jak i zewnętrznym serwisom | Prod / test |
| SOZ | System obsługi zgłoszeń zbieranych od użytkowników wskazanych portali informacyjnych i następnie procesowanie tych zgłoszeń. | Prod / test |
| Konto (Baza Wiedzy) | Moduł pozwalający użytkownikom zarejestrować się w serwisie biznes.gov.pl oraz pozwalający im na zarządzanie swoimi danymi powiązanymi z ich kontem. | Prod / test |
| Logowanie (Baza Wiedzy) | Moduł odpowiedzialnym za autentykację użytkowników serwisu | Prod / test |
| CI/CD | Środowisko dostarczania i integracji Systemu \*.biznes.gov.pl  Moduł dostępny z wyznaczonych sieci. | Prod |
| Zulip | Platforma do komunikacji w departamencie, projektach i umowach prowadzonych przez departament. | Prod |
| Redmine | Oprogramowanie do zarządzania projektem | Prod / test |
| Media serwer | Serwer multimediów w portalu | Prod / test |
| Poczta | Serwer pocztowy w systemie | Prod / test |
| Projekty | Serwer świadczący usługi związane z utrzymaniem design Systemu dla nowych formularzy CEIDG | Prod |
| SVN | Repozytorium plików projektu związanego z budową, utrzymaniem i rozwojem Systemu | Prod |
| Styleguide | Zbiór makiet, wzorców graficznych, praktyk użyty do tworzenia stron interfejsów graficznych dla użytkowników Systemu we wszystkich aplikacjach Systemu | Prod |
| Static | Serwer plików statycznych do Systemu | Prod / test |
| eDoręczenia | Moduł konta przedsiębiorcy do realizacji eDoręczeń | Prod / test |
| Wyszukiwarka firm | Front wyszukiwania firm w rejestrach CEIDG oraz KRS | Prod / test |

Infrastruktura utrzymująca system obejmuje (według stanu na dzień publikacji ogłoszenia):

System został zbudowany w oparciu o sprzęt serwerowy o architekturze kasetowej, sprzęt sieciowy zapewniający komunikację w ramach sieci LAN i WAN oraz realizujący ochronę przed nieuprawnionym dostępem i atakami sieciowymi. Dostarczone zostały również systemy pomocnicze:

1. Zarządzanie wirtualizacją

2. Kopie bezpieczeństwa

3. Monitorowanie i administracji

1. CEIDG i Hurtownia Danych

*CEIDG*

Zgodnie z obowiązującymi przepisami, minister właściwy do spraw gospodarki przy użyciu systemów teleinformatycznych prowadzi: Centralną Ewidencję i Informację o Działalności Gospodarczej (art. 2 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy) oraz Punkt Informacji dla Przedsiębiorcy (art. 51 ust. 1 ww. ustawy). Wpis, zmiana oraz wykreślenie przedsiębiorcy z CEIDG może się odbywać za pośrednictwem systemu CEIDG lub za pośrednictwem systemu Punktu Informacji dla Przedsiębiorcy (art. 3 ust. 1 ustawy z dnia 6 marca 2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy).

Zadaniem CEIDG jest:

1. ewidencjonowanie przedsiębiorców będących osobami fizycznymi;

2. udostępnianie informacji o przedsiębiorcach oraz innych podmiotach w zakresie wskazanym w ustawie;

3. udostępnianie informacji o zakresie i terminie zmian we wpisach do CEIDG oraz w informacjach i danych udostępnianych w CEIDG, a także o wprowadzającym te zmiany podmiocie;

4. umożliwienie wglądu do danych bezpłatnie udostępnianych przez Centralną Informację Krajowego Rejestru Sądowego;

5. udostępnianie informacji o ustanowionym pełnomocniku lub prokurencie, w tym o zakresie udzielonego pełnomocnictwa lub o rodzaju i sposobie wykonywania prokury.

Minister właściwy do spraw gospodarki przechowuje i przetwarza dane oraz informacje związane z realizacją zadań wynikających z ustawy, w szczególności w związku z przyjmowaniem żądań, zgłoszeń, wniosków i zmian w Rejestrze CEIDG.

Poniższa tabela prezentuje moduły funkcjonalne CEIDG:

|  |  |
| --- | --- |
| Moduł | Przeznaczenie i integracje |
| Rejestr CEIDG | Przeznaczenie: Elektroniczny rejestr działający w ramach Systemu Teleinformatycznego Centralnej Ewidencji i Informacji o Działalności Gospodarczej, którego przeznaczeniem jest: ewidencjonowanie przedsiębiorców będących osobami fizycznymi; udostępnianie informacji o przedsiębiorcach i innych podmiotach w zakresie wskazanym w ustawie; umożliwienie wglądu do danych bezpłatnie udostępnianych przez Centralną Informację Krajowego Rejestru Sądowego: umożliwienia ustalenia terminu i zakresu zmian wpisów w CEIDG oraz wprowadzającego je organu. |
| API rejestru CEIDG | Przeznaczenie: wielofunkcyjny interfejs programistyczny zapewniający dostęp do danych z rejestru CEIDG oraz realizujący dwukierunkową wymianę danych pomiędzy organami uczestniczącymi w procesie zakładania działalności gospodarczej, organami prowadzącymi rejestry działalności regulowanej oraz innymi podmiotami przekazującymi dane do CEIDG na podstawie odrębnych porozumień. |
| Replika dla hurtowni danych i systemu CEIDG | Przeznaczenie: mechanizm repliki transakcyjnej MS SQL dla danych z rejestru CEIDG służący do zasilenia Hurtowni Danych. |
| Aplikacja urzędnika | Przeznaczenie: aplikacja udostępniona przez przeglądarkę internetową (aplikacja webowa) umożliwiającą urzędnikom realizacje zadań w procesach realizowanych przez CEIDG, m.ni. rejestracja i potwierdzanie konta urzędnika, składanie wniosków do CEIDG, przekazanie informacji dot. wpisu do rejestrów działalności regulowanej, wyszukiwarka przedsiębiorców, podgląd danych, wykonywanie raportów. |

*Hurtownia Danych*

Hurtownia Danych CEIDG i Biznes.gov.pl jest jednym z elementów ekosystemu Biznes.gov.pl. Użytkownicy mogą korzystać z usług po uprzednim uwierzytelnieniu się w serwisie Biznes.gov.pl.

W skład Hurtowni Danych wchodzą trzy aplikacje webowe:

- Interfejs API (Gravitee) służący do administrowania interfejsem ,

- Aplikacja Raportowa (Wyn Enterprise) służąca do administrowania i generowania raportów,

- Aplikacja Monitorowania Przepływów Danych (Havran) służąca do oceny parametrów jakościowych i ilościowych transferów danych Hurtowni.

Możliwość skorzystania z poszczególnych aplikacji oraz funkcji uzależniona jest od ról, które są dostępne dla konkretnego, uwierzytelnionego Użytkownika.

Poniższy schemat prezentuje Hurtownię Danych i jej otoczenie:



Poniższa tabela prezentuje modułu funkcjonalne Hurtowni Danych:

|  |  |
| --- | --- |
| Moduł | Przeznaczenie i integracje |
| Interfejs API | Moduł realizujący usługi dostępu do danych z Repliki bazy CEIDG oraz Bazy Hurtowni Danych za pośrednictwem API (application programming interface). Integralną częścią Interfejsu API jest moduł administracyjny służący do zarządzania API. |
| Aplikacja raportowania | Aplikacja umożliwiająca tworzenie oraz wyświetlanie raportów bazujących na danych Bazy Hurtowni Danych. Aplikacja służy również do zarządzania źródłami, zbiorami danych, szablonami raportów, regułami dystrybucji raportów, itp. |
| Aplikacja Monitorowania Przepływów Danych | Aplikacja przeznaczona dla Administratorów do monitorowania procesów ETL. |
| Replika Bazy CEiDG | Replika operacyjnej bazy danych Rejestru CEIDG, aktualizowana na bieżąco (tzw. replika transakcyjna); stanowi bezpośrednie źródło danych biznesowych dla Interfejsu API oraz Bazy Hurtowni Danych, jak również jest źródłem informacji o rolach urzędników dla Aplikacji Raportowej. |
| Baza Hurtowni Danych (Analityczna) | Główna baza danych zasilająca Aplikację Raportową, w której składowane są dane z Repliki Bazy CEIDG w formie zoptymalizowanej pod kątem raportowania |

Poniższa tabela prezentuje strukturę modułów interfejsu API Hurtowni Danych:

|  |  |
| --- | --- |
| Moduł | Przeznaczenie i integracji |
| API Gateway | Umożliwia nakładanie limitów na przesyłanie danych lub liczby zapytań w wybranym okresie czasu. Udziela dostępu do poszczególnych usług API lub odmawia dostępu w przypadku podania niezgodnego tokenu JWT. Pozwala na zarządzanie dostępem i użytkownikami API poprzez moduł API Management. Użytkownik może subskrybować wybrane API. Konieczna jest rejestracja użytkownika w API Gateway (poprzez udostępnioną usługę REST API w ramach API Gateway). Rejestracja jest dokonywana w Biznes.gov.pl w momencie generowania tokenu JWT dla użytkownika. |
| API | Zdefiniowano pięć usług zapewniających realizację wyszukiwania podmiotów w Replice bazy CEIDG oraz bezpośrednio w systemie zewnętrznym eKRS za pośrednictwem Wyszukiwarki KRS. API będzie łączyło wyniki znalezione w Replice bazy CEIDG oraz otrzymane przez WebService Wyszukiwarka KRS. Pozostałe usługi do pobierania listy raportów oraz konkretnego raportu będą wykorzystywały do tego Aplikację Raportową działającą w ramach Hurtowni Danych CEIDG. |
| API MSWF | Zdefiniowano pięć usług:  Wyszukiwarka prosta umożliwia poprzez podanie w języku naturalnym zapytania i otrzymania wyników najbardziej zbliżonych do zapytania  Wyszukiwanie zaawansowane umożliwia przeszukiwanie zasobów CEIDG oraz eKRS przy użyciu zamkniętego katalogu kryteriów wyszukiwawczych.  Pobieranie informacji o wskazanych wpisach z CEIDG lub eKRS.  Pobieranie na podstawie unikalnego numeru KRS informacji zgromadzonych w CEIDG na temat koncesji, zezwoleń, licencji oraz wpisów do rejestrów działalności regulowanej jak również kwalifikacjach zawodowych w kontekście podmiotu zarejestrowanego w eKRS.  Pobieranie historii zmian zachodzących we wpisach pochodzących z CEIDG. |
| Repozytorium Aplikacji Zarządzania API | Zawiera informacje o kontach użytkowników, subskrypcje do API, konfigurację limitów ilości żądań dla użytkowników. |
| Replika bazy CEIDG | Replika operacyjnej bazy danych Rejestru CEIDG, aktualizowana na bieżąco (tzw. replika transakcyjna); stanowi bezpośrednie źródło danych biznesowych dla Interfejsu API oraz Bazy Hurtowni Danych, jak również jest źródłem informacji o rolach urzędników dla Aplikacji. |
| eKRS | Serwis eKRS to serwis prowadzony przez Ministerstwo Sprawiedliwości udostępniający dokumenty i informacje z Krajowego Rejestru Sądowego (KRS). Dane i informacje z eKRS udostępniane są poprzez API i stronę internetową https://ekrs.ms.gov.pl/. Usługi eKRS umożliwiają wyszukiwanie podmiotów z rejestru KRS. |

Z punktu widzenia dostępności Systemu CEIDG wykorzystywane są dwie Instancje: Instancja w Ośrodku Podstawowym będąca rozproszonym klastrem HA (dwie lokalizacje) i Instancja w Ośrodku Zapasowym. Instancje w Ośrodku Podstawowym i Zapasowym współpracują w trybie Active-Passive.

System CEIDG wykorzystuje w Ośrodku Podstawowym infrastrukturę sprzętową oferowaną jako usługi IaaS i PaaS.

Zakłada się, że czas przełączenia pomiędzy ośrodkami w przypadku wystąpienia Awarii wynosi nie więcej niż 24 godziny.

1. Ośrodek Podstawowy CEIDG. Dwie lokalizacje geograficzne, w których jest eksploatowana Instancja produkcyjna Systemu CEIDG.

2. Ośrodek Zapasowy więcej niż jedna lokalizacji geograficznych, w których eksploatowane są:

3. instancja zapasowa Systemu (replika instancji produkcyjnej Systemu CEIDG),

4. instancja testowa Systemu CEIDG,

5. instancja deweloperska Systemu CEIDG.

6. systemy zewnętrzne z którymi integruje się System CEIDG,

7. systemy uruchomione w lokalizacji Wykonawcy to Portal Serwisowy, którego elementem jest System Monitorowania Stanu systemów.

1. Narzędzie do tworzenia ankiet i system CRM projektu Innopoint

Na projekt Innopoint składają się systemy informatyczne służące do stworzenia profilu przedsiębiorcy i dopasowanie do niego programu oferowanego w ramach Funduszy Europejskich.

1. System klasy CRM (customer relationship management) spełniający następujące wymagania:

- posiada moduł raportowy,

- jest zintegrowany z infolinią oraz czatem w zakresie automatycznej rejestracji zgłoszeń,

- posiada konfigurowalną bazę wiedzy/zagadnień

1. Baza danych przedsiębiorców utrzymywana przez dostawcę usług infolinii i systemu CRM

- udostępnia API dla systemu CRM w zakresie danych przedsiębiorców (interfejs API wykonany i opisany zgodnie z wymaganiami Ministra Cyfryzacji (https://dane.gov.pl/pl/article/standard-interfejsu-programistycznego-aplikacji-api)).

- posiada moduł umożliwiający generowanie raportów

- baza danych musi zapewniać rozliczalność poprzez rejestrację wszystkich wykonywanych operacji (z zapisem min. czasu wykonania operacji, rodzaju operacji, użytkownika lub systemu dokonującego operacji),

- baza danych musi zapewnić mechanizmy tworzenia kopii zapasowych dla danych oraz mechanizm odtwarzania danych z kopii zapasowych,

1. Autorskie narzędzie do tworzenia ankiet, spełniające następujące wymagania:

- udostępnia formularz rezerwacji wizyty w punkcie prewypełniany danymi uzupełnianymi w ankiecie,

- jest zintegrowane z API Hurtowni Danych / CEIDG w zakresie pobierania danych o przedsiębiorstwie na podstawie NIP

- wypełnione ankiety zasilają bazę danych przedsiębiorców

- posiada panel administracyjny dla użytkowników o specjalnych przywilejach

Systemy są utrzymywane przez podmioty wyłonione w drodze przetargów publicznych.

1. Planowane zmiany lub nowe funkcjonalności w obrębie systemów Biznes.gov.pl, CEIDG i Hurtowni Danych

Zamawiający realizuje lub będzie realizował projekty współfinansowane ze środków Unii Europejskiej polegające na modyfikacji badanych systemów. W latach 2025 – 2027 przewidziano szereg prac modernizacyjnych w obrębie udostępnianych e-usług i funkcjonalności systemów Biznes.gov.pl oraz CEIDG wraz z Hurtownią Danych. Przewiduje się również konieczność testowania/audytowania projektowanych zmian. Prace będą zlecane w ramach prawa opcji. Poniżej zaprezentowano wysokopoziomowy opis planowanych modyfikacji:

- przepięcie wybranych e-usług publicznych realizowanych poprzez Biznes.gov.pl z kanału transmisyjnego ePUAP na kanał e-Doręczeń. W związku z realizacją tego zadania przewiduje się przede wszystkim zmiany wykonywane w modułach: silnika procesów e-usług, silnika e-usług (frontend), konfiguratora e-usług, aplikacji e-Doręczeń oraz Konta.

- dodanie nowych metod e-płatności (karty, BLIK). W związku z realizacją tego zadania przewiduje się przede wszystkim zmiany wykonywane w modułach Biznes.gov.pl: konfiguratora e-usług, silnika e-usług (frontend) oraz aplikacji Konta.

- modyfikacja layoutu systemu Biznes.gov.pl w oparciu o nowy styleguide. W związku z realizacją tego zadania przewiduje się przede wszystkim zmiany wykonywane w modułach Biznes.gov.pl: silnika e-usług (frontend), aplikacji e-Doręczeń oraz Konta.

- dodanie możliwości obsługiwania dokumentacji kadrowej w Koncie Przedsiębiorcy. W związku z realizacją tego zadania przewiduje się przede wszystkim zmiany wykonywane w modułach: silnika procesów e-usług, silnika e-usług (frontend), konfiguratora e-usług, aplikacji Konta. Ponadto przewiduje się rozbudowę systemu CEIDG w zakresie dodania możliwości obsługi pełnomocnictw do powyższych e-usług. Potencjalnie przewiduje się również możliwość utworzenia nowego API Hurtowni Danych lub CEIDG do obsługi w systemie umów.

- wyłączenie dotychczasowego modułu Zaplecza i przeniesienie jego funkcjonalności do SMC Biznes.gov.pl. Nowa aplikacja zostanie zbudowana w architekturze mikrofrontendów. Każdy moduł w aplikacji Zaplecza będzie oddzielnym modułem z własnym API. API Nowego Zaplecza będzie się komunikowało poprzez proxy zgodnie z protokołem starego API Zaplecza. Nie przewiduje się zmian w mechanizmach logowania.

- udostępnienie nowych funkcjonalności w ramach modułu Twoja firma aplikacji mObywatel. W ramach tego zadania przewiduje się modyfikację systemu CEIDG w zakresie mikroserwisów udostępniających e-usługi.

- udostępnienie na portalu Biznes.gov.pl dedykowanej sekcji o roboczej nazwie „Bezpieczna Firma”, w ramach którego działać będą usługi analityczne oraz prekwalifikacyjne i preweryfikacyjne w kontekście zaleceń NIS2. Przewiduje się w związku z tym przede wszystkim zmiany w zakresie silnika e-usług (frontend) oraz aplikacji Konta.

1. Inne systemy Ministerstwa

Przewiduje się również możliwość realizacji prac testowania (testy penetracyjne) lub audytu innych systemów teleinformatycznych Zamawiającego. Zlecane zadania w tym zakresie mogą dotyczyć przede wszystkim: mechanizmów uwierzytelniania, zarządzania sesją, skuteczności walidacji danych, stosowanych algorytmów kryptograficznych, obsługi błędów, zapewnienia ochrony danych i bezpieczeństwa komunikacji, wykrywania usług sieciowych, ochrony przed przeciążeniem systemów, bezpieczeństwa urządzeń i sieci. W tym zakresie przewiduje się przede wszystkim zastosowanie testów penetracyjnych typu black-box.

**Szczegółowa dokumentacja poszczególnych systemów, o których mowa w pkt. a) – c) może zostać udostępniona do wglądu w siedzibie Zamawiającego w terminie pomiędzy publikacją ogłoszenia a terminem składania ofert, po uprzednim złożeniu przez wnioskującego Wykonawcę oświadczenia o zachowaniu poufności.**

1. Opis i zakres czynności audytowych

Poniższa tabela prezentuje maksymalny wysokopoziomowy zakres prac audytowych w odniesieniu do danego systemu:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Czynność | Biznes.gov.pl | CEIDG i Hurtownia Danych | Narzędzia Innopoint | Inne  (prawo opcji – wybrane czynności) |
| Testy bezpieczeństwa / testy penetracyjne | X | X | X | X |
| Analiza zagrożeń i podatności | X | X | X | X |
| Analiza kodu źródłowego | X | X |  | X |
| Audyt infrastruktury | X | X |  | X |
| Audyt bezpieczeństwa przetwarzania danych i ochrony danych | X | X | X | X |
| Analiza architektury sieciowej | X | X |  | X |
| Analiza bezpieczeństwa konfiguracji urządzeń i aplikacji | X | X | X | X |
| Analiza funkcjonowania systemów bezpieczeństwa | X | X |  | X |
| Audyt wydajności | X | X | X | X |

Szczegółowy zakres danych czynności audytowych zostanie ustalony na etapie zlecenia danego zadania lub zlecenia w ramach prawa opcji.

1. Testy bezpieczeństwa / testy penetracyjne

Czynność polega na przeprowadzeniu testów penetracyjnych i symulowanych ataków (wg najnowszych wytycznych OWASP wymienionych na liście TOP10 aktualnej na dzień realizacji audytu) obejmujących:

* testy bezpieczeństwa aplikacji pod kątem, m.in.:

- ataków semantycznych na adres URL,

* 1. - ataków związanych z ładowaniem plików,
  2. - ataków typu Cross-Site Scripting,
  3. - ataków typu Cross-Site Request Forgery,
  4. - ataków typu MITM (Man in the Middle),
  5. - ataków typu Cross Site Tracing,
  6. - ataków typu Session Hijacking / Session Fixation,
  7. - ataków typu Forced Browsing,
  8. - ujawnienia kodu/ścieżki dostępu (Path Disclousure),
  9. - ujawnienia parametrów ograniczających (Parameter Delimiter)
  10. - podrabiania zarządzania formularza,
  11. - sfałszowania żądania http,
  12. - ujawnienia danych przechowywanych w bazie,
  13. - trawersowania katalogów (Path Traversal),
  14. - ujawniania kodu źródłowego,
  15. - przepełnienia bufora lub stosu,
  16. - wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection),
  17. - niepożądanego przekierowania,
  + badania enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu,
  + badania możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu
  + badania możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskania dostępu do systemu
  + badania możliwości zablokowania dostępu do systemu wszystkim lub wybranym użytkownikom,
  + badania możliwości usunięcia lub modyfikacji danych w systemie.

1. Analiza zagrożeń i podatności

Czynność polega na:

* Analizie wdrożeń rozwiązań informatycznych obszaru monitorowania bezpieczeństwa IT,
* Detekcji błędów aplikacyjnych,
* Recenzji architektury logicznej,
* Analizie podatności w zainstalowanej wersji serwera,
* Skanowaniu podatności w udostępnionych usługach sieciowych,
* Detekcji podatności w udostępnionych aplikacjach webowych.

1. Analiza kodu źródłowego

Czynność polega na analizie wskazanego przez Zamawiającego kodu źródłowego lub jego wycinka celem zidentyfikowania:

* Niewspieranych lub niebezpiecznych bibliotek,
* Naruszeń licencyjnych,
* Nieprawidłowo działającej architektury,
* Zagrożeń bezpieczeństwa wynikających z zastosowanego kodu.

1. Audyt infrastruktury

Czynność polega na wykonaniu następujących analiz:

- analiza wersji oprogramowania pod kątem znanych podatności,

- analiza konfiguracji dostępu do urządzeń,

- przegląd konfiguracji dot. użytkowników korzystających z urządzeń, prawa dostępu, listy

- testy słabych haseł,

- analiza konfiguracji i reguł VPN,

- analiza wykorzystanych mechanizmów kryptograficznych,

- analiza zasad filtracji ruchu sieciowego,

- analiza pod kątem obecności niepożądanych usług,

- analiza mechanizmów logowania zdarzeń.

1. Audyt bezpieczeństwa przetwarzania danych i ochrony danych

Czynność polega na przeprowadzeniu audytu bezpieczeństwa przetwarzania danych zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności oraz zgodnie z normami: ISO 27001 „Technika informatyczna. Techniki Bezpieczeństwa. systemu zarządzania bezpieczeństwem informacji. Wymagania” i ISO 27002 „Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji”.

W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z 5 sierpnia 2010 (Dz. U. z 2010 r. nr 182, poz. 1228).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowane systemy powinny zagwarantować:

a. poufność – zabezpieczenie danych przed ich udostępnieniem nieuprawnionemu odbiorcy,

b. integralność – zabezpieczenie danych przed modyfikacją lub zniekształceniem przez nieuprawnionych użytkowników,

c. rozliczalność – określenie i weryfikowanie odpowiedzialności za wykorzystanie systemu,

d. autentyczność – weryfikacje tożsamości podmiotów i prawdziwości zasobów,

e. niezawodność – gwarancja oczekiwanego zachowania systemu.

Audyt obejmuje sprawdzenie aktualnego stanu przetwarzania danych osobowych zarówno pod kątem zagadnień technicznych, organizacyjnych oraz prawnych ze szczególnym uwzględnieniem wymagań opisanych w ustawie o ochronie danych osobowych.

Maksymalny zakres czynności audytowych:

a. Przegląd i analiza dokumentacji, w tym analiza dokumentacji polityk bezpieczeństwa i procedur, pod kątem zgodności z wymaganiami (w zakresie jak wyżej) Rozporządzenia, ze szczególnym uwzględnieniem zagadnień IT.

b. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.

1. Analiza architektury sieciowej

Czynność obejmuje:

W zakresie architektury sieciowej

- weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),

- określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),

- poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),

- weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,

- weryfikacja dostępu do Internetu z LAN,

- szczegółowa analiza komunikacji sieciowej,

- weryfikacja zasad utrzymania sieci,

- analiza wersji oprogramowania pod kątem znanych podatności (firmware),

- analiza konfiguracji dostępu do urządzenia,

- przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,

- analiza konfiguracji i reguł VPN,

- analiza wykorzystanych mechanizmów kryptograficznych,

- analiza zasad filtracji ruchu sieciowego,

- analiza pod kątem obecności niepożądanych usług,

- analiza mechanizmów logowania zdarzeń

W zakresie brzegu sieci:

- weryfikacja topologii/architektury sieci,

- testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu, próby tunelowania, oprogramowania typu exploit, kontrola aplikacji, ataki ogólnego typu bez predefiniowanych sygnatur, ruchu generowanego przez szkodliwe oprogramowanie, podatności serwera i klienta wraz z możliwością definiowania własnych sygnatur, regularności aktualizacji firewall w celu przeciwdziałania nowym zagrożeniom, itp.)

- ogólna analiza komunikacji sieciowej z poziomu sieci Internet,

- skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach,

- wykrywanie usług sieciowych udostępnionych w sieci Internet,

- próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet,

- testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service” co najmniej 2 metodami zaproponowanymi przez Wykonawcę,

- testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.

1. Analiza bezpieczeństwa konfiguracji urządzeń i aplikacji

Czynność polega na:

analizie zgodności konfiguracji i sposobu funkcjonowania urządzeń w tym przede wszystkim:

- weryfikacja udostępnionych usług sieciowych,

- weryfikacja zbędnych usług wraz ze wskazaniem ich podatności,

- weryfikacja zaimplementowanych systemów aktualizacji,

- weryfikacja zaimplementowanych systemów logowania zdarzeń,

- weryfikacja mechanizmów administracji zdalnej,

- weryfikacja przypisania użytkowników do właściwych grup,

- weryfikacja uprawnień zgodnie z pryncypium jak najmniejszych uprawnień (ang. „least privilige”),

- przeprowadzenie prób obejścia uprawnień i uzyskania nieautoryzowanego dostępu do informacji,

- weryfikacja sposobu udostępniania baz danych na poziomie sieciowym,

- analiza implementacji podstawowych zasad hardeningowych bazy danych (np. wyłączenie nieużywanych usług, wyłączenie nieużywanych metod dostępu, konfiguracja uprawnień do obiektów, logowanie zdarzeń, składowanie logów, monitorowanie dostępu do obiektów, monitorowanie instrukcji języka SQL),

- analiza architektury baz danych (np. wykorzystanie mechanizmów autoryzacji oraz uwierzytelniania, segmentacja uprawnień, wykorzystywanie widoków, wykorzystywanie procedur składowych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych),

- analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych),

- analiza użytych technologii.

Analizie podatności aplikacji:

- wytypowanie wrażliwych punktów w aplikacji,

- inspekcja mechanizmów uwierzytelniania / autoryzacji,

- zabezpieczenia interfejsu użytkownika za pomocą captcha oraz za pomocą zweryfikowanego certyfikatu, two-factor authentication (2FA)

- weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych,

- weryfikacja obsługi błędów,

- analiza poziomu bezpieczeństwa oferowanego przez aplikacje.

1. Analiza funkcjonowania systemów bezpieczeństwa

Czynność polega na:

analizie i ocenie funkcjonowania następujących systemów bezpieczeństwa:

- System antywirusowy.

- System antyspamowy.

- System DLP (Data Leak Prevention/Data Loss Prevention).

- System Firewall.

- System backupowy wraz z testem odtworzenia systemu z backupu (Zamawiający nie wymaga odtwarzania systemu na zasobach Wykonawcy), ocena lokalizacji baz danych zawierających kopie bezpieczeństwa (bezpieczeństwo ośrodka, ośrodek zapasowy).

- System zasilania awaryjnego.

1. Audyt wydajności

Czynność obejmuje testy serwera www: dla jednoczesnych sesji: 0…5000 (maksymalnie) – pomiar czasów odpowiedzi serwera i czasu załadowania strony. Czasy odpowiedzi i ładowania maja obejmować wartości średnie i maksymalne dla każdego punktu pomiarowego.

1. Zakres prac realizowanych w ramach prawa opcji

Zamawiający ma prawo do skorzystania z prawa opcji w postaci zleceń wskazujących zakres wykonywanych czynności audytowych w odniesieniu do zadań określonych w rozdz. I pkt. 4-5 OPZ. Zakres zlecanych czynności nie będzie wykraczał ponad zdefiniowane w pkt a) – i) powyżej. Czasochłonność danego zlecenia będzie wyceniana przez Wykonawcę każdorazowo po wskazaniu przez Zamawiającego zakresu tego zlecenia i będzie podlegała akceptacji Zamawiającego.

Łączna liczba roboczogodzin przeznaczonych na realizację prawa opcji nie może przekroczyć 500.

1. Opis procesu realizacji zadań i wyniki prac
2. Zadania audytowe

Dotyczy zadań opisanych w rozdz. I pkt 1-3.

Orientacyjny harmonogram realizacji poszczególnych zadań znajduje się w rozdz. V, przy czym terminy te mogą ulec zmianie. Zlecenie będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia czynności oraz obszar podlegający audytowi/testom.

Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu, w terminie 14 dni liczonych od dnia otrzymania zlecenia, przedstawi Zamawiającemu szczegółową propozycję Planu audytu/testów wydajności. Zamawiający po otrzymaniu propozycji planu, w terminie 7 dni liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do planu, bądź dokona jego zatwierdzenia. W przypadku zgłoszenia uwag, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) przedstawienia przez Wykonawcę poprawionego planu. Następnie jeśli Wykonawca przedstawi poprawiony plan, Zamawiający w terminie 7 dni kalendarzowych może dokonać zatwierdzenia go, a jeśli poprzednio zgłoszone uwagi nie zostały w pełni uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi. Wykonawca przystąpi do wykonywania audytu/testów nie wcześniej niż w dniu zatwierdzenia planu.

Czynności audytowe/testowe dla danego zadania nie mogą trwać dłużej niż 45 dni kalendarzowych. Po zakończeniu realizacji zadania, w terminie nie dłuższym niż 7 dni kalendarzowych liczonych od jego zakończenia, Wykonawca przedstawi Zamawiającemu Raport z wykonanego zadania. Zamawiający w terminie 7 dni kalendarzowych liczonych od dnia otrzymania raportu, przedstawi Wykonawcy ewentualne uwagi do wykonanych prac, bądź dokona zatwierdzenia raportu. W przypadku zgłoszenia uwag do raportu, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) na prawidłowe wykonanie raportu. W przypadku raportu, co do którego zostały zgłoszone uwagi, Zamawiający w terminie 7 dni kalendarzowych dokona zatwierdzenia poprawionego przez Wykonawcę raportu, a jeśli poprzednio zgłoszone uwagi nie zostały uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi.

Rozliczeniu podlegają wyłącznie zadania zatwierdzone przez Zamawiającego.

1. Zlecenia w ramach prawa opcji

Dotyczy zadań opisanych w rozdz. I pkt. 4-5.

Zamawiający wystawi Zlecenie na realizację zadania lub części zadania, które będzie zawierać m. in. proponowaną datę rozpoczęcia i zakończenia prac oraz zakres prac. Zadania te będą rozliczane w ramach puli roboczogodzin przysługujących do wykorzystania w ramach umowy, przy czym realizacja danego zadania lub jego części nie może prowadzić do przekroczenia tej puli.

Wykonawca uwzględniając wymagania oraz informacje zawarte w zleceniu w terminie 7 dni liczonych od daty otrzymania zlecenia przedstawi Zamawiającemu Propozycję realizacji zadania (lub jego części) wraz ze wskazaniem pracochłonności (wyrażonej w roboczogodzinach) potrzebnej na jego wykonanie. Zamawiający po otrzymaniu propozycji, w terminie 7 dni kalendarzowych liczonych od dnia jej otrzymania, przedstawi Wykonawcy ewentualne uwagi do propozycji, bądź dokona jej zatwierdzenia. W przypadku zgłoszenia uwag Zamawiający wskaże termin, nie krótszy niż 3 dni robocze, na przedstawienie przez Wykonawcę poprawionej propozycji realizacji zlecenia. Następnie jeśli Wykonawca przedstawi poprawioną propozycję realizacji zlecenia, Zamawiający w terminie 7 dni kalendarzowych może dokonać zatwierdzenia jej, a jeśli poprzednio zgłoszone uwagi nie zostały w pełni uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi z terminem. Wykonawca przystąpi do wykonania prac na podstawie propozycji zatwierdzonej przez Zamawiającego.

Proponowany termin wykonania prac zostanie określony w zleceniu przez Zamawiającego. Faktyczny termin realizacji zostanie wskazany przez Wykonawcę w Propozycji realizacji zlecenia, przy czym termin ten nie może być dłuższy niż 30 dni kalendarzowych. Wykonawca najpóźniej w ostatnim dniu realizacji danego zlecenia Wykonawca przedstawi Zamawiającemu Zamawiający w terminie 7 dni liczonych od dnia otrzymania raportu, przedstawi Wykonawcy ewentualne uwagi do wykonanych prac, bądź dokona zatwierdzenia raportu. W przypadku zgłoszenia uwag do raportu, zamawiający wskaże termin (nie krótszy, niż 3 dni robocze) na prawidłowe wykonanie raportu. W przypadku raportu, co do którego zostały zgłoszone uwagi, Zamawiający w terminie 7 dni kalendarzowych dokona zatwierdzenia poprawionego przez Wykonawcę raportu, a jeśli poprzednio zgłoszone uwagi nie zostały uwzględnione przez Wykonawcę, wtedy Zamawiający może ponownie zgłosić uwagi Raport z wykonanego zlecenia.

Rozliczeniu podlegają wyłącznie zlecenia, których realizacja została zatwierdzona przez Zamawiającego. Zamawiający będzie realizował płatności za wykonane zlecenia każdorazowo po ich wykonaniu. Podstawę stanowić będą zatwierdzone raporty. Zamawiający ma prawo do rezygnacji z realizacji danego zlecenia w dowolnym momencie przed jego zatwierdzeniem, bez podania przyczyny.

1. Wymagania dotyczące współpracy Zamawiającego z Wykonawcą

Zamawiający dopuszcza możliwość przeprowadzenia prac audytowych w formie zdalnej. W przypadku konieczności przeprowadzenia audytu stacjonarnego, jego zakres zostanie ustalony z Zamawiającym na etapie realizacji audytu. W takim przypadku Wykonawca uzyska dostęp do infrastruktury w zakresie ustalonym z Zamawiającym.

Serwerownie znajdują się w okolicach Warszawy, Katowic lub innych miejscowości na terenie Polski – Wykonawca musi uwzględniać możliwość wykonywania podróży służbowych w celu realizacji audytu stacjonarnego, w ramach wynagrodzenia, które otrzyma.

Zamawiający nie dopuszcza możliwości włączenia maszyny Wykonawcy do sieci w audytowanej infrastrukturze.

W ramach współpracy Wykonawca i Zamawiający wyznaczają w swoich strukturach osobę prowadzącą zadanie lub zlecenie oraz osobę zastępującą. Wykonawca zobowiązany jest do sprawnej i terminowej realizacji zamówienia oraz stałej współpracy z Zamawiającym, w tym:

- pozostawania w stałym kontakcie (kontakt telefoniczny oraz drogą elektroniczną; spotkania z Zamawiającym w miarę potrzeb; wyznaczenie osoby do kontaktów roboczych);

- informowania o stanie prac, pojawiających się problemach i innych zagadnieniach istotnych dla realizacji badania.

d) Procedura odbiorowa

W terminie 7 dni od dnia zrealizowania danego zadania lub części zadania w ramach zlecenia Wykonawca sporządzi protokół odbioru zadania i przekaże go Zamawiającemu do akceptacji. Protokół powinien być podpisany przez obie Strony lub osoby przez nie upoważnione. Protokół odbioru zadania lub części zadania w ramach zlecenia powinien zawierać w szczególności:

a) dzień i miejsce wystawienia i odbioru zadania,

b) oświadczenie Zamawiającego, o braku lub istnieniu zastrzeżeń lub nieprawidłowości w realizacji zadania,

c) podpisy Stron lub osób upoważnionych.

W razie uchylania się Wykonawcy od sporządzenia protokołu w uzgodnionym terminie, Zamawiający może samodzielnie sporządzić protokół odbioru zadania lub jego części i treść takiego protokołu uznać za zaakceptowaną przez Wykonawcę.

Zadanie w ramach prawa opcji zostaje uznane za zrealizowane w przypadku zakończenia umowy lub wyczerpania puli roboczogodzin przeznaczonych na to zadanie, przy czym Wykonawcy przysługuje z tego tytułu wynagrodzenie wyłącznie w wysokości odpowiadającej liczbie roboczogodzin wynikającej z udzielonych przez Zamawiającego zleceń.

1. Prognozowany harmonogram prac

1. Wykonanie audytu bezpieczeństwa i wydajności systemu Biznes.gov.pl – Q2/Q3 2025 r.

2. Wykonanie audytu bezpieczeństwa i wydajności systemów CEIDG i Hurtowni Danych – Q2/Q3 2025 r.

3. Przeprowadzenie testów penetracyjnych oraz wydajności narzędzia do tworzenia ankiet i systemu CRM funkcjonujących w ramach projektu Innopoint – Q1/Q2 2025 r.

4. Przeprowadzenie testów w zakresie bezpieczeństwa i wydajności przed wdrażaniem zmian lub nowych funkcjonalności w obrębie systemów Biznes.gov.pl, CEIDG i Hurtowni Danych – prawo opcji - realizowane w trybie ciągłym, nie później niż 24 miesiące od dnia podpisania umowy.

5. Realizacja doraźnych zleceń wsparcia w zakresie cyberbezpieczeństwa dot. systemów teleinformatycznych MRiT – prawo opcji - realizowane w trybie ciągłym, nie później niż 24 miesiące od dnia podpisania umowy.

1. Załączniki

Szczegółowa dokumentacja audytowanych systemów - załączniki mogą zostać udostępnione do wglądu w siedzibie Zamawiającego po uprzednim złożeniu oświadczenia o poufności.