Projekt

Platforma Internetowa Polityki Zakupowej Państwa

Opis Przedmiotu Zamówienia

Audyt Platformy Internetowej Polityki Zakupowej Państwa w zakresie cyberbezpieczeństwa, bezpieczeństwa przetwarzania danych, wydajności systemu teleinformatycznego wraz z usługami wsparcia eksperckiego inżyniera ds. cyberbezpieczeństwa.

Ministerstwo Rozwoju i Technologii

Warszawa, 2024 r.

SPIS TREŚCI

1. WSTĘP

Przedmiotem zamówienia jest wykonanie audytów cyberbezpieczeństwa, wydajności systemu teleinformatycznego, bezpieczeństwa przetwarzania danych oraz usługę wsparcia eksperckiego inżyniera ds. cyberbezpieczeństwa IT i inżyniera ds. wydajności infrastruktury IT zgodnie ze specyfikacją w poszczególnych rozdziałach.

Przyjęta przez Radę Ministrów Polityka zakupowa państwa (link https://www.gov.pl/web/rozwoj-technologia/polityka-zakupowa-panstwa2) w jednym ze swych programów zobowiązuje ministra wł. ds. gospodarki do budowy platformy internetowej. Platforma ma być atrakcyjnym i centralnym źródłem wiedzy z zakresu zamówień publicznych. Dzięki niej kompleksowa i darmowa wiedza o zamówieniach publicznych będzie łatwo i szybko dostępna zarówno dla zainteresowanych wykonawców, w tym z sektora MŚP, jak i dla wszystkich innych praktyków zamówień publicznych.

Moduły podstawowe podlegające testom:

1. Moduł środowisko uruchomieniowe: będzie główną stroną startową Platformy Internetowej Polityki Zakupowej Państwa, zawierającą treści wynikającego z zawartości poszczególnych modułów funkcjonalnych, umożliwiającą jednocześnie wybór poprzez parametryzację przez użytkownika wyświetlanych treści.
2. Moduł repozytorium Wiedzy: będzie zapewniał dostęp do wszystkich materiałów, wytycznych oraz dobrych praktyk, w tym tych przygotowanych przez UZP, z zakresu zamówień publicznych.
3. Moduł forum: będzie miejscem prowadzenia szerokiej dyskusji na temat zamówień publicznych. Umożliwi ono praktykom wymianę wiedzy i doświadczenia. Wpłynie to na lepsze zrozumienie i efektywne wykorzystanie zamówień publicznych. Forum dostępne będzie dla wszystkich uczestników rynku zamówień publicznych.
4. Moduł orzecznictwo: umożliwi bezpłatny i przyjazny dostęp do orzecznictwa, w tym Krajowej Izby Odwoławczej, z obszaru zamówień publicznych. Dzięki temu praktycy zamówień publicznych będą mogli rozszerzać swoją wiedzę.
5. Moduł kontrola: zapewni organom kontroli możliwość szybkiej i łatwiej wymiany informacji o wynikach przeprowadzonych kontroli udzielania zamówień, co przyczyni się do zwiększenia transparentności i skuteczności procesów kontrolnych. Baza wyników kontroli będzie dostępna także dla osób niebędących kontrolerami.
6. Moduł konsorcjum: zapewni możliwość zamieszczania ogłoszeń, dzięki którym przedsiębiorcy, w tym przede wszystkim MŚP, będą mogli znaleźć partnerów do realizacji zamówień publicznych. Dzięki temu przedsiębiorcy będą mieli łatwiejszy dostęp do rynku zamówień publicznych.

Moduły **opcjonalne** podlegające testom:

1. Moduł e-learning: znajdą się na nim szkolenia w formie e-learning, obejmujące najważniejsze elementy z obszaru zamówień publicznych. Dzięki temu uczestnicy będą mogli pogłębić swoją wiedzę i umiejętności - w elastyczny sposób i w dogodnym dla siebie czasie.
2. Moduł webinarium: zapewni możliwość organizowania i prowadzenia warsztatów i szkoleń online z obszaru zamówień publicznych. Na szkoleniach tych wykładowcy i eksperci będą mogli dzielić się wiedzą i doświadczeniem z wykonawcami oraz przedsiębiorcami. Dzięki temu dostęp do wiedzy będzie łatwiejszy i wygodniejszy.
3. Moduł certyfikacja: po wejściu w życie przepisów o certyfikacji wykonawców zamówień publicznych zapewniony zostanie dostęp do wydanych certyfikatów, co ułatwi przedsiębiorcom posługiwanie się nimi. Przedsiębiorca nie będzie bowiem musiał składać certyfikatu zamawiającemu, gdyż zamawiający będzie mógł samodzielnie pobrać certyfikat z bazy.

2. CEL ZAMÓWIENIA

Celem audytu jest weryfikacja zgodności Platformy Internetowej Polityki Zakupowej Państwa z wymaganiami:

1. Zgodność z wymaganiami Krajowych Ram Interoperacyjności.
2. Zgodność z Narodowymi Standardami Cyberbezpieczeństwa (NSC).
3. Zgodność z regulacjami wewnętrznymi MRiT:
   - Polityką bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa.
   - Zasadami projektowania i wytwarzania bezpiecznych systemów i oprogramowania.
   - Zasadami zarzadzania danymi uwierzytelniającymi.
   - Polityką Bezpieczeństwa Informacji.

- Zasadami bezpieczeństwa informacji w Ministerstwie Rozwoju i Technologii.

Celem audytu są ponadto:

- wykonanie prac związanych ze zbadaniem wewnętrznych i zewnętrznych podatności i wynikających z nich zagrożeń wraz z oceną poziomu bezpieczeństwa,
- weryfikacja poziomu zapewnienia zasobów do monitorowania bezpieczeństwa systemów,
- dostarczenie wniosków, zaleceń, rekomendacji w celu dokładnego rozpoznania i redukcji wskazanych podatności oraz wskazanie adekwatnych działań mających na celu wyeliminowanie zagrożeń.

Po zakończeniu czynności audytowych Wykonawca jest zobowiązany do przedstawienia opracowania eksperckiego w formie raportu (szczegóły w części poświęconej Raportom).

3. ZAKRES ZAMÓWIENIA

Przedmiotem zamówienia jest wykonanie audytów cyberbezpieczeństwa, wydajności systemu teleinformatycznego, bezpieczeństwa przetwarzania danych oraz usługi wsparcia eksperckiego inżyniera bezpieczeństwa IT zgodnie ze specyfikacją w poszczególnych rozdziałach.

Zamówienie zostało podzielone na VI zadań:

3.1. ZAKRES ZADANIA I

1. Przeprowadzenie audytu cyberbezpieczeństwa Platformy Internetowej Polityki Zakupowej Państwa dla modułów funkcjonalnych (Moduły: środowisko uruchomieniowe, repozytorium wiedzy, forum, kontrole, konsorcjum, wyszukiwarka orzeczeń KIO).
2. Analiza koncepcji architektury teleinformatycznej Platformy, jej komponentów i użytych systemów i narzędzi teleinformatycznych pod kątem cyberbezpieczeństwa.
3. Audyt bezpieczeństwa przetwarzania danych.
4. W przypadku wykrycia nieprawidłowości w pierwszej iteracji Zamawiający zleci wykonanie retestu po usunięciu wykrytych podatności a także wykonanie weryfikacji dokumentacji. Retesty będą zlecane w zależności od potrzeb w ramach prawa opcji. Zamówienia na kolejne retesty będą realizowane oddzielnie. W ofercie należy przedstawić wyceny jednostkowe dla poszczególnych typów retestu.

3.1.1. ZAKRES CZYNNOŚCI

3.1.1.1. ZAKRES CZYNNOŚCI DLA AUDYTU INFRASTRUKTURY TELEINFORMATYCZNEJ MRIT DEDYKOWANEJ BEZPOŚREDNIO PLATFORMIE

1. analiza konfiguracji dostępu do urządzeń teleinformatycznych;
2. przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł;
3. analiza konfiguracji i reguł VPN;
4. analiza wykorzystanych mechanizmów kryptograficznych;
5. analiza zasad filtracji ruchu sieciowego;
6. analiza pod kątem obecności niepożądanych usług;
7. analiza mechanizmów logowania zdarzeń;
8. analiza pod kątem wydawania kolejnych wersji oprogramowania w środowisku CI/CD GitLab.

3.1.1.2. ZAKRES CZYNNOŚCI DLA AUDYTU CZĘŚCI WEBOWEJ SYSTEMU

Walidacja danych wejściowych w tym:

1. pliki cookie;
2. nagłówki.

Parametry wysyłane metodami http:

1. badanie sesji użytkowników aplikacji,
2. badanie komunikatów błędów,
3. badanie mechanizmów przekierowań,
4. badanie danych zapisywanych do bazy danych,
5. badanie integralności logów aplikacji,
6. szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS),
7. badanie błędów logicznych aplikacji w miejscach krytycznych.

Badanie środowiska pracy aplikacji:

1. uprawnień w systemie plików oraz zasobów,
2. wersji usług,
3. użytego oprogramowania podnoszącego poziom bezpieczeństwa,
4. architektury systemu dotyczącej wszelkich obszarów bezpieczeństwa (składowanie logów, obsługa wyjątków itd.),
5. konfiguracji serwerów, z których korzysta aplikacja pod kątem bezpieczeństwa.

3.1.1.3. ZAKRES CZYNNOŚCI DLA AUDYTU KONFIGURACJI SYSTEMÓW OPERACYJNYCH I BAZ DANYCH

1. analiza architektury i technologii platformy;
2. analiza konfiguracji serwera (+uprawnień plików/katalogów);
3. analiza architektury i technologii bazy danych;
4. analiza konfiguracji aplikacji bazy danych;
5. analiza dostępu do bazy danych, uprawnień;
6. analiza mechanizmów logowania;
7. analiza możliwych ataków.

3.1.1.4. ZAKRES CZYNNOŚCI DLA AUDYTU ARCHITEKTURY SIECIOWEJ DEDYKOWANEJ BEZPOŚREDNIO PLATFORMIE

1. weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
2. weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
3. weryfikacja dostępu do Internetu z LAN,
4. szczegółowa analiza komunikacji sieciowej,
5. weryfikacja zasad utrzymania sieci,
6. analiza wersji oprogramowania pod kątem znanych podatności (firmware),
7. analiza konfiguracji dostępu do urządzenia,
8. przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
9. analiza konfiguracji i reguł VPN,
10. analiza wykorzystanych mechanizmów kryptograficznych,
11. analiza zasad filtracji ruchu sieciowego,
12. analiza pod kątem obecności niepożądanych usług,
13. analiza mechanizmów logowania zdarzeń

3.1.1.5. ZAKRES CZYNNOŚCI DLA ANALIZY BRZEGU SIECI DEDYKOWANEJ BEZPOŚREDNIO PLATFORMIE

1. weryfikacja topologii/architektury sieci,
2. testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu,
3. 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.);
4. ogólna analiza komunikacji sieciowej z poziomu sieci Internet;
5. skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach;
6. wykrywanie usług sieciowych udostępnionych w sieci Internet;
7. próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet;
8. testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service" co najmniej 2 metodami zaproponowanymi przez Wykonawcę;
9. testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.

3.1.1.6. ZAKRES CZYNNOŚCI DLA AUDYTU BEZPIECZEŃSTWA I KONFIGURACJI SYSTEMÓW IT (URZĄDZEŃ I APLIKACJI) DEDYKOWANYCH BEZPOŚREDNIO PLATFORMIE

1. analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
    - 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 składowanych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych);
    - analiza komunikacji z klientami bazodanowymi (mechanizmy kryptograficzne, transfery danych).
2. analiza podatności aplikacji:
    - wytypowanie wrażliwych punktów w aplikacji;
    - inspekcja mechanizmów uwierzytelniania / autoryzacji;
    - zabezpieczenia interfejsu użytkownika;
    - weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych;

- weryfikacja obsługi błędów;
- analiza poziomu bezpieczeństwa oferowanego przez aplikacje.

3.1.1.7. ZAKRES CZYNNOŚCI DLA PRZEPROWADZENIE TESTÓW PENETRACYJNYCH I SYMULOWANYCH ATAKÓW

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

1. testy bezpieczeństwa aplikacji pod kątem, m.in.:
   - ataków semantycznych na adres URL;
   - ataków związanych z ładowaniem plików;
   - ataków typu Cross-Site Scripting;
   - ataków typu Cross-Site Request Forgery;
   - ataków typu MITM (Man in the Middle);
   - ataków typu Cross Site Tracing;
   - ataków typu Session Hijacking / Session Fixation;
   - ataków typu Forced Browsing;
   - ujawnienia kodu/ścieżki dostępu (Path Disclousure);
   - ujawnienia parametrów ograniczających (Parameter Delimiter);
   - podrabiania zarządzania formularza;
   - sfałszowania żądania http;
   - ujawnienia danych przechowywanych w bazie;
   - trawersowania katalogów (Path Traversal);
   - ujawniania kodu źródłowego;
   - przepełnienia bufora lub stosu;
   - wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection);
   - niepożądanego przekierowania;
2. badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu;
3. badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu;
4. badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
5. badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom;
6. badanie możliwości modyfikacji/usunięcia danych z systemu.

3.1.1.8. ZAKRES CZYNNOŚCI DLA AUDYTU FUNKCJONOWANIA SYSTEMÓW BEZPIECZEŃSTWA DEDYKOWANYCH BEZPOŚREDNIO PLATFORMIE

Audyt obejmuje analizę i ocenę funkcjonowania następujących systemów bezpieczeństwa:

1. System antywirusowy.
2. System antyspamowy.
3. System DLP (Data Leak Prevention/Data Loss Prevention).
4. System Firewall.
5. 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).
6. .

7. I w innych obszarach wskazanych przez Wykonawcę w obszarze cyberbezpieczeństwa (jeśli Wykonawca uważa, że jest to niezbędne do kompleksowego przeprowadzenia zakresu prac wraz z jego uzasadnieniem).

Zakres czynności audytu:

1. Kompleksowa analiza skuteczności działania.
2. Analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
3. Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
4. Weryfikacja i/lub opracowanie wskaźników efektywności.
5. I innych zakresów wskazanych przez Wykonawcę w obszarze cyberbezpieczeństwa (jeśli Wykonawca uważa, że jest to niezbędne do kompleksowego przeprowadzenia zakresu prac wraz z jego uzasadnieniem).

3.1.1.9. ZAKRES CZYNNOŚCI DLA AUDYTU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Audyt bezpieczeństwa przetwarzania danych będzie realizowany zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773) oraz zgodnie z normami z serii ISO 27001 i ISO 27002.
W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2024 r. poz. 632).
W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowany system powinien 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 – gwarancję oczekiwanego zachowania systemu;
f) dostępność - informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu

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

Zakres czynności dla audytu bezpieczeństwa przetwarzania danych

1. 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.
2. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.
3. Weryfikacja kwalifikacji personelu odpowiedzialnego za bezpieczeństwo badanych systemów oraz przestrzegania procedur.

3.1.2. RAPORTOWANIE WYNIKÓW TESTÓW I PRAC

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty zawierające minimalnie:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów);
2. opis ryzyk i propozycji planów zarządzania ryzykami

3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi;
4. wyniki działań, testów i ich interpretacja, w szczególności:
   - informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie liczbę stwierdzonych nieprawidłowości w podziale na systemy i krytyczności;
   - opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność;
   - Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w audytowanych obszarach systemu w ramach zadania I wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanej platformy (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy infrastruktury teleinformatycznej platformy w celu podniesienia bezpieczeństwa i jego wydajności.
10. podsumowanie/streszczenie dla kierownictwa
11. szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

3.2. ZAKRES ZADANIA II (PRAWO OPCJI)

1. Przeprowadzenie audytu cyberbezpieczeństwa Platformy Internetowej Polityki Zakupowej Państwa dla modułów, które będą rozszerzeniem o dodatkowe funkcjonalności w stosunku do badanych w zadaniu I zamówienia (Zamawiający planuje rozbudowę o nowe funkcjonalności Platformy Internetowej Polityki Zakupowej Państwa, stąd potrzeba wykonania dodatkowych testów. Dodatkowe moduły funkcjonalne **mogą być wdrożone pojedynczo lub w grupie**. Dodatkowe moduły:
   1.1. e-learning,
   1.2. webinary,
   1.3. certyfikacja wykonawców.

   W ofercie należy podać wycenę przeprowadzenia audytu cyberbezpieczeństwa dla pojedynczego modułu funkcjonalnego.

   W przypadku wykrycia nieprawidłowości w pierwszej iteracji zostaną wykonane retesty po usunięciu wykrytych podatności a także wykonanie weryfikacji dokumentacji. Retesty będą zlecane w zależności od potrzeb w ramach prawa opcji.

   Zamówienia na kolejne retesty będą realizowane oddzielnie. W ofercie należy przedstawić wyceny jednostkowe dla poszczególnych typów retestu.

2. Analiza koncepcji architektury teleinformatycznej Platformy pod kątem cyberbezpieczeństwa dla nowych komponentów:
   2.1. e-learning,
   2.2. webinary,
   2.3. certyfikacja wykonawców.

   W ofercie należy przedstawić wyceny jednostkowe analizy koncepcji architektury osobno dla każdego modułu funkcjonalnego.

3.2.1. ZAKRES CZYNNOŚCI

3.2.1.1. ZAKRES CZYNNOŚCI DLA AUDYTU INFRASTRUKTURY TELEINFORMATYCZNEJ MRIT DEDYKOWANEJ BEZPOŚREDNIO PLATFORMIE

1. analiza pod kątem obecności niepożądanych usług;
2. analiza mechanizmów logowania zdarzeń.

3.2.1.2. ZAKRES CZYNNOŚCI DLA AUDYTU CZĘŚCI WEBOWEJ SYSTEMU

Walidacja danych wejściowych w tym:

1. pliki cookie;
2. nagłówki.

Parametry wysyłane metodami http:

1. badanie sesji użytkowników aplikacji,
2. badanie komunikatów błędów,
3. badanie mechanizmów przekierowań,
4. badanie danych zapisywanych do bazy danych,
5. badanie integralności logów aplikacji,
6. szukanie funkcjonalności potencjalnie niebezpiecznych pod kątem wykorzystywanych zasobów (DoS).

Badanie środowiska pracy aplikacji:

1. uprawnień w systemie plików oraz zasobów,
2. wersji usług,
3. użytego oprogramowania podnoszącego poziom bezpieczeństwa.

3.2.1.3. ZAKRES CZYNNOŚCI DLA AUDYTU KONFIGURACJI SYSTEMÓW OPERACYJNYCH I BAZ DANYCH

1. analiza dostępu do bazy danych, uprawnień;
2. analiza możliwych ataków.

3.2.1.4. ZAKRES CZYNNOŚCI DLA AUDYTU ARCHITEKTURY SIECIOWEJ

1. weryfikacja sieci LAN na strefy sieciowe (w tym wykorzystanie urządzeń typu firewall oraz VLAN),
2. określenie usług działających w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
3. poszukiwanie podatności w wybranych podsieciach (do 10 podsieci – nie więcej niż 15 hostów dla jednego systemu),
4. weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI,
5. weryfikacja dostępu do Internetu z LAN,
6. szczegółowa analiza komunikacji sieciowej,
7. weryfikacja zasad utrzymania sieci,
8. analiza wersji oprogramowania pod kątem znanych podatności (firmware),
9. analiza konfiguracji dostępu do urządzenia,

10. przegląd konfiguracji dot. użytkowników korzystających z urządzenia, praw dostępu, list dostępów, testy słabych haseł,
11. analiza konfiguracji i reguł VPN,
12. analiza wykorzystanych mechanizmów kryptograficznych,
13. analiza zasad filtracji ruchu sieciowego,
14. analiza pod kątem obecności niepożądanych usług,
15. analiza mechanizmów logowania zdarzeń

3.2.1.5. ZAKRES CZYNNOŚCI DLA ANALIZY BRZEGU SIECI

1. weryfikacja topologii/architektury sieci,
2. testy szczelności systemów klasy firewall (w tym działania funkcji IPS obsługującej w czasie rzeczywistym zagrożenia typu nadużycie protokołu,
3. 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.);
4. ogólna analiza komunikacji sieciowej z poziomu sieci Internet;
5. skanowanie portów różnymi technikami, w celu wykrycia potencjalnych luk bezpieczeństwa w udostępnianych usługach;
6. wykrywanie usług sieciowych udostępnionych w sieci Internet;
7. próba detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniach dostępnych z sieci Internet;
8. testowanie odporności usług wystawionych do sieci Internet na ataki „Denial of Service" co najmniej 2 metodami zaproponowanymi przez Wykonawcę;
9. testowanie odporności usług wystawionych do sieci Internet, za pomocą narzędzi eksploatujących typowe luki bezpieczeństwa.

3.2.1.6. ZAKRES CZYNNOŚCI DLA AUDYTU BEZPIECZEŃSTWA I KONFIGURACJI SYSTEMÓW IT (URZĄDZEŃ I APLIKACJI)

3. analiza zgodności konfiguracji i sposobu funkcjonowania urządzeń:
    - 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 składowanych, przechowywanie oraz dostęp do danych wrażliwych, przechowywanie oraz dostęp do danych audytowych, szyfrowanie danych);

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

4. analiza podatności aplikacji:
   - wytypowanie wrażliwych punktów w aplikacji;
   - inspekcja mechanizmów uwierzytelniania / autoryzacji;
   - zabezpieczenia interfejsu użytkownika;
   - weryfikacja implementacji mechanizmów ochronnych dla serwerów aplikacyjnych;
   - weryfikacja obsługi błędów;
   - analiza poziomu bezpieczeństwa oferowanego przez aplikacje.

3.2.1.7. ZAKRES CZYNNOŚCI DLA PRZEPROWADZENIA TESTÓW PENETRACYJNYCH I SYMULOWANYCH ATAKÓW

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

7. testy bezpieczeństwa aplikacji pod kątem, m.in.:
   - ataków semantycznych na adres URL;
   - ataków związanych z ładowaniem plików;
   - ataków typu Cross-Site Scripting;
   - ataków typu Cross-Site Request Forgery;
   - ataków typu MITM (Man in the Middle);
   - ataków typu Cross Site Tracing;
   - ataków typu Session Hijacking / Session Fixation;
   - ataków typu Forced Browsing;
   - ujawnienia kodu/ścieżki dostępu (Path Disclousure);
   - ujawnienia parametrów ograniczających (Parameter Delimiter);
   - podrabiania zarządzania formularza;
   - sfałszowania żądania http;
   - ujawnienia danych przechowywanych w bazie;
   - trawersowania katalogów (Path Traversal);
   - ujawniania kodu źródłowego;
   - przepełnienia bufora lub stosu;
   - wstrzykiwania kodu wykonywalnego innych języków programowania (np. SQL Injection / JSON Injection);
   - niepożądanego przekierowania;
8. badanie enumeracji i wykorzystania znanych podatności w celu uzyskania nieautoryzowanego dostępu;
9. badanie możliwości podszywania się pod użytkowników i uzyskania nieautoryzowanego dostępu do systemu;
10. badanie możliwości podszywania się pod użytkowników uprzywilejowanych i uzyskanie dostępu do systemu
11. badanie możliwości blokowania/umożliwienia dostępu do systemu wszystkim lub wybranym jej użytkownikom;
12. badanie możliwości modyfikacji/usunięcia danych z systemu.

3.2.1.8. ZAKRES CZYNNOŚCI DLA AUDYTU FUNKCJONOWANIA SYSTEMÓW BEZPIECZEŃSTWA

Audyt obejmuje analizę i ocenę funkcjonowania następujących systemów bezpieczeństwa:

8. System antywirusowy.

9. System antyspamowy.
10. System DLP (Data Leak Prevention/Data Loss Prevention).
11. System Firewall.
12. 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).
13. I w innych obszarach wskazanych przez Wykonawcę w obszarze cyberbezpieczeństwa (jeśli Wykonawca uważa, że jest to niezbędne do kompleksowego przeprowadzenia zakresu prac wraz z jego uzasadnieniem).

Zakres czynności audytu:

6. Kompleksowa analiza skuteczności działania.
7. Analizę procedur utrzymaniowych i monitorowania systemów bezpieczeństwa.
8. Weryfikacja poprawności konfiguracji systemów bezpieczeństwa.
9. Weryfikacja i/lub opracowanie wskaźników efektywności.
10. I innych zakresów wskazanych przez Wykonawcę w obszarze cyberbezpieczeństwa (jeśli Wykonawca uważa, że jest to niezbędne do kompleksowego przeprowadzenia zakresu prac wraz z jego uzasadnieniem).

3.2.1.9. ZAKRES CZYNNOŚCI DLA AUDYTU BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Audyt bezpieczeństwa przetwarzania danych będzie realizowany zgodnie z wymaganiami wymienionymi w rozporządzeniu Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2024 r. poz. 773) oraz zgodnie z normami z serii ISO 27001 i ISO 27002.

W audytowanych systemach nie będą przetwarzane dane niejawne w rozumieniu ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2024 r. poz. 632).

W obszarze zapewnienia bezpieczeństwa przetwarzanych danych oraz ochrony danych, audytowany system powinien 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 – gwarancję oczekiwanego zachowania systemu,
f) dostępność - informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu

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

Zakres czynności dla audytu bezpieczeństwa przetwarzania danych

1. 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.
2. Weryfikacja zgodności systemów z wymaganiami Rozporządzenia (w zakresie jak wyżej), ze szczególnym uwzględnieniem zagadnień IT.
3. Weryfikacja kwalifikacji personelu odpowiedzialnego za bezpieczeństwo badanych systemów oraz przestrzegania procedur.

3.2.2. RAPORTOWANIE WYNIKÓW TESTÓW I PRAC

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty zawierające minimalnie:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów);
2. opis ryzyk i propozycji planów zarządzania ryzykami;
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi;
4. wyniki działań, testów i ich interpretacja, w szczególności:
   - informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie liczbę stwierdzonych nieprawidłowości w podziale na systemy i krytyczności;
   - opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność;
   - Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. Rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa i jego wydajności.
10. Podsumowanie/streszczenie dla kierownictwa
11. Szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

3.3. ZAKRES ZADANIA III

1. Przeprowadzenie audytu wydajności Platformy Internetowej Polityki Zakupowej Państwa dla modułów funkcjonalnych (Moduły: środowisko uruchomieniowe, repozytorium wiedzy, forum, kontrole, konsorcjum, wyszukiwarka orzeczeń KIO).

3.3.1. CEL I ZAKRES AUDYTU WYDAJNOŚCI SYSTEMU

Cele Testów Wydajności

- Ocena zachowania systemu pod różnym obciążeniem.
- Identyfikacja potencjalnych wąskich gardeł.
- Analiza i ocena możliwości, że system może obsłużyć przewidywaną liczbę użytkowników.
- Określenie maksymalnego obciążenia, które system może wytrzymać.
- Ocena wpływu zmian w konfiguracji systemu na wydajność systemu.

Zakres audytu wydajności dla systemu

W ramach zakresu testów wydajności Wykonawca jest zobowiązany do przeprowadzenia testów zarówno w środowisku FrontEnd, jak i BackEnd. Testy te mają obejmować ocenę wydajności interfejsu użytkownika, logiki aplikacyjnej, oraz komunikacji z bazą danych. Wyniki testów powinny być przedstawione w szczegółowym

raporcie dla każdego rodzaju testów z listy poniżej i zawierającym wnioski oraz rekomendacje dotyczące optymalizacji.

3.3.2. RODZAJE TESTÓW DO WYKONANIA

3.3.2.1. TESTY OBCIĄŻENIOWE (LOAD TESTING)

1. Symulacja rzeczywistych warunków użytkowania systemu.
2. Testowanie systemu przy różnych poziomach obciążenia (np. 100, 500, 1000 jednoczesnych użytkowników).
3. Pomiar czasu odpowiedzi na kluczowe zapytania i operacje.

3.3.2.2. TESTY PRZECIĄŻENIOWE (STRESS TESTING)

1. Testowanie systemu poza jego normalnymi granicami operacyjnymi.
2. Identyfikacja punktu, w którym system zaczyna się degradować.
3. Obserwacja, jak system odzyskuje sprawność po usunięciu nadmiernego obciążenia.

3.3.2.3. TESTY WYDAJNOŚCIOWE (PERFORMANCE TESTING)

1. Pomiar czasu odpowiedzi i przepustowości systemu przy ustalonym obciążeniu.
2. Ocena wydajności poszczególnych komponentów systemu (np. serwera aplikacyjnego, bazy danych).

3.3.2.4. TESTY SKALOWALNOŚCI (SCALABILITY TESTING)

1. Ocena, jak wydajność systemu zmienia się w miarę zwiększania obciążenia.
2. Testowanie, czy system może być łatwo rozbudowany w celu obsługi większej liczby użytkowników.

3.3.2.5. TESTY WYTRZYMAŁOŚCIOWE (ENDURANCE TESTING)

1. Długotrwałe testowanie systemu pod stałym obciążeniem.
2. Identyfikacja problemów związanych z przeciekami pamięci lub degradacją wydajności w czasie.

3.3.3. ZADANIA I CZYNNOŚCI

3.3.3.1. PRZYGOTOWANIE ŚRODOWISK DO AUDYTU

1. Weryfikacja środowisk pod kątem gotowości do startu testów
2. Konfiguracja narzędzi do monitorowania wydajności

3.3.3.2. TESTY FRONT END I BACK END

1. Logowanie i uwierzytelnianie użytkowników**:** Pomiar czasu logowania, obsługa błędnych logowań.
2. Przeglądanie i wyszukiwanie danych: Pomiar czasu odpowiedzi na zapytania wyszukiwania.
3. Operacje CRUD (Create, Read, Update, Delete): Pomiar czasu odpowiedzi na operacje na danych.
4. Generowanie raportów: Ocena wydajności podczas generowania prostych i złożonych raportów.
5. Obsługa plików: Testowanie uploadu i downloadu załączników różnej wielkości.

3.3.3.3. TESTY DLA SERWERA APLIKACYJNEGO

1. Zarządzanie sesjami użytkowników: Testowanie obsługi dużej liczby jednoczesnych sesji.
2. Skalowalność aplikacji: Testowanie, jak aplikacja reaguje na zwiększenie liczby użytkowników.
3. Zarządzanie zasobami: Monitorowanie zużycia pamięci, CPU i innych zasobów systemowych.

3.3.3.4. TESTY DLA BAZY DANYCH

1. Wydajność zapytań: Pomiar czasu wykonania kluczowych zapytań do bazy danych.
2. Obciążenie bazy danych: Testowanie wydajności bazy danych przy dużej liczbie równoczesnych zapytań.
3. Konsystencja danych: Testowanie zachowania bazy danych podczas intensywnych operacji zapisu i odczytu.

3.3.3.5. BEZPIECZEŃSTWO I ODSEPAROWANIE

1. Testy bezpieczeństwa: ocena czy środki zabezpieczające nie wpływają negatywnie na wydajność systemu.
2. Odseparowanie komponentów: Upewnienie się, że serwer aplikacyjny i baza danych działają poprawnie z zastosowanymi zabezpieczeniami.

3.3.4. RAPORTOWANIE WYNIKÓW TESTÓW I PRAC

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty zawierające minimalnie:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów);
2. opis ryzyk i propozycji planów zarządzania ryzykami;
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi;
4. wyniki działań, testów i ich interpretacja, w szczególności:
   - informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie liczbę stwierdzonych nieprawidłowości w podziale na systemy i krytyczności;
   - opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność;
   - Informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa i jego wydajności.
10. podsumowanie/streszczenie dla kierownictwa
11. szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

3.4. ZAKRES ZADANIA IV (PRAWO OPCJI)

1. Przeprowadzenie audytu wydajności Platformy Internetowej Polityki Zakupowej Państwa dla modułów, które będą rozszerzeniem o dodatkowe funkcjonalności podlegające audytom wskazane w zadaniu II zamówienia, (Zamawiający planuje rozbudowę o nowe funkcjonalności Platformy Internetowej Polityki Zakupowej Państwa, stąd potrzeba wykonania dodatkowych testów). Dodatkowe moduły funkcjonalne **mogą być wdrożone pojedynczo lub w grupie.** Dodatkowe moduły funkcjonalne:
   1.1 e-learning,
   1.2 webinary,
   1.3 certyfikacja wykonawców.

W ofercie należy podać wycenę przeprowadzenia audytu cyberbezpieczeństwa dla pojedynczego modułu funkcjonalnego.

3.4.1. CEL I ZAKRES AUDYTU WYDAJNOŚCI SYSTEMU

Cele Testów Wydajności

- Ocena zachowania systemu pod różnym obciążeniem.
- Identyfikacja potencjalnych wąskich gardeł.
- Zapewnienie, że system może obsłużyć przewidywaną liczbę użytkowników.
- Określenie maksymalnego obciążenia, które system może wytrzymać.
- Ocena wpływu zmian w konfiguracji systemu na wydajność systemu.

Zakres audytu wydajności dla systemu

W ramach zakresu testów wydajności Wykonawca jest zobowiązany do przeprowadzenia testów zarówno w środowisku FrontEnd, jak i BackEnd. Testy te mają obejmować ocenę wydajności interfejsu użytkownika, logiki aplikacyjnej, oraz komunikacji z bazą danych. Wyniki testów powinny być przedstawione w szczegółowym raporcie dla każdego rodzaju testów z listy poniżej i zawierającym wnioski oraz rekomendacje dotyczące optymalizacji.

3.4.2. RODZAJE TESTÓW DO WYKONANIA

3.4.2.1. TESTY OBCIĄŻENIOWE (LOAD TESTING)

1. Symulacja rzeczywistych warunków użytkowania systemu.
2. Testowanie systemu przy różnych poziomach obciążenia (np. 100, 500, 1000 jednoczesnych użytkowników).
3. Pomiar czasu odpowiedzi na kluczowe zapytania i operacje.

3.4.2.2. TESTY PRZECIĄŻENIOWE (STRESS TESTING)

1. Testowanie systemu poza jego normalnymi granicami operacyjnymi.
2. Identyfikacja punktu, w którym system zaczyna się degradować.
3. Obserwacja, jak system odzyskuje sprawność po usunięciu nadmiernego obciążenia.

3.4.2.3. TESTY WYDAJNOŚCIOWE (PERFORMANCE TESTING)

1. Pomiar czasu odpowiedzi i przepustowości systemu przy ustalonym obciążeniu.

2. Ocena wydajności poszczególnych komponentów systemu (np. serwera aplikacyjnego, bazy danych).

3.4.2.4. TESTY SKALOWALNOŚCI (SCALABILITY TESTING)

1. Ocena, jak wydajność systemu zmienia się w miarę zwiększania obciążenia.
2. Testowanie, czy system może być łatwo rozbudowany w celu obsługi większej liczby użytkowników.

3.4.2.5. TESTY WYTRZYMAŁOŚCIOWE (ENDURANCE TESTING)

1. Długotrwałe testowanie systemu pod stałym obciążeniem.
2. Identyfikacja problemów związanych z przeciekami pamięci lub degradacją wydajności w czasie.

3.4.3. ZADANIA I CZYNNOŚCI

3.4.3.1. PRZYGOTOWANIE ŚRODOWISK DO AUDYTU

1. Weryfikacja środowisk pod kątem gotowości do startu testów
2. Konfiguracja narzędzi do monitorowania wydajności

3.4.3.2. TESTY FRONT END I BACK END

1. Logowanie i uwierzytelnianie użytkowników**:** Pomiar czasu logowania, obsługa błędnych logowań.
2. Przeglądanie i wyszukiwanie danych: Pomiar czasu odpowiedzi na zapytania wyszukiwania.
3. Operacje CRUD (Create, Read, Update, Delete): Pomiar czasu odpowiedzi na operacje na danych.
4. Generowanie raportów: Ocena wydajności podczas generowania prostych i złożonych raportów.
5. Obsługa plików: Testowanie uploadu i downloadu załączników różnej wielkości.

3.4.3.3. TESTY DLA SERWERA APLIKACYJNEGO

1. Zarządzanie sesjami użytkowników: Testowanie obsługi dużej liczby jednoczesnych sesji.
2. Skalowalność aplikacji: Testowanie, jak aplikacja reaguje na zwiększenie liczby użytkowników.
3. Zarządzanie zasobami: Monitorowanie zużycia pamięci, CPU i innych zasobów systemowych.

3.4.3.4. TESTY DLA BAZY DANYCH

1. Wydajność zapytań: Pomiar czasu wykonania kluczowych zapytań do bazy danych.
2. Obciążenie bazy danych: Testowanie wydajności bazy danych przy dużej liczbie równoczesnych zapytań.
3. Konsystencja danych: Testowanie zachowania bazy danych podczas intensywnych operacji zapisu i odczytu.

3.4.3.5. BEZPIECZEŃSTWO I ODSEPAROWANIE

1. Testy bezpieczeństwa: Ocena czy środki zabezpieczające nie wpływają negatywnie na wydajność systemu.

2. Odseparowanie komponentów: Upewnienie się, że serwer aplikacyjny i baza danych działają poprawnie z zastosowanymi zabezpieczeniami.

3.4.4. RAPORTOWANIE WYNIKÓW TESTÓW I PRAC

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty zawierające minimalnie:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów);
2. opis ryzyk i propozycji planów zarządzania ryzykami;
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi;
4. wyniki działań, testów i ich interpretacja, w szczególności:
   - informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie liczbę stwierdzonych nieprawidłowości w podziale na systemy i krytyczności;
   - opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność;
   - informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa i jego wydajności.
10. podsumowanie/streszczenie dla kierownictwa
11. Szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

3.5. ZAKRES ZADANIA V (PRAWO OPCJI)

1. Wykonawca zobowiązany jest do udzielania wsparcia eksperckiego w kwestiach związanych z cyberbezpieczeństwem, wydajnością systemu i jakością tworzonego lub utrzymywanego oprogramowania w zakresie m.in.:
   1.1. wdrożeń rozwiązań informatycznych obszaru monitorowania cyberbezpieczeństwa IT;
   1.2. analizy zagrożeń zewnętrznych i wewnętrznych w obszarze cyberbezpieczeństwa IT;
   1.3. detekcji błędów aplikacyjnych;
   1.4. recenzji architektury logicznej;
   1.5. analizy podatności występujących w zainstalowanej wersji serwera;
   1.6. skanowania podatności w udostępnionych usługach sieciowych;
   1.7. detekcji podatności w udostępnionych aplikacjach webowych (np. próby ominięcia ekranów logowania, kradzież danych z aplikacji);
   1.8. próby eskalacji ataku na pozostałe maszyny, systemy w LAN po przejęciu kontroli nad jedną z aplikacji;
   1.9. analizy kodu źródłowego aplikacji;
2. Jako wynik prac Wykonawca jest zobowiązany do opracowania oceny eksperckiej i przedstawienia w formie raportu.

3. Planowany wymiar liczby świadczonych roboczogodzin wsparcia eksperckiego 200.

3.5.1. RAPORTOWANIE WYNIKÓW TESTÓW I PRAC

W wyniku przeprowadzonych prac Wykonawca dostarczy raporty zawierające minimalnie:

1. opis przeprowadzonych działań (w tym weryfikacji dokumentacji i wykonanych testów);
2. opis ryzyk i propozycji planów zarządzania ryzykami;
3. propozycja uruchomienia dodatkowych mechanizmów bezpieczeństwa umożliwiających ochronę przed możliwymi atakami sieciowymi i aplikacyjnymi;
4. wyniki działań, testów i ich interpretacja, w szczególności:
   - informacje dotyczące ogólnej oceny poziomu bezpieczeństwa oraz odporności na ataki badanych systemów zawierające podsumowanie liczbę stwierdzonych nieprawidłowości w podziale na systemy i krytyczności;
   - opis lokalizacji wykrytych podatności - sposobu, w jaki można zlokalizować i powtórzyć testowy atak na podatność;
   - informacje na temat poziomu ochrony realizowanego przez system zabezpieczeń
5. opis technicznych znalezionych podatności w obu obszarach wraz z zaleceniami i rekomendacjami mającymi na celu zminimalizowanie bądź całkowitą redukcję ryzyka związanego z wykrytymi podatnościami
6. identyfikacja tzw. wąskich gardeł
7. wnioski z audytu, działań (określenie ilościowego i jakościowego poziomu niebezpieczeństwa podatności)
8. Rekomendacje i zalecenia pozwalające na usunięcie wykrytych słabości, a tym samym podniesienie poziomu bezpieczeństwa badanych systemów (określenia sposobu naprawy wykrytych podatności w tym zmian konfiguracyjnych)
9. rekomendacje w zakresie rozbudowy systemu informatycznego w celu podniesienia bezpieczeństwa i jego wydajności.
10. podsumowanie/streszczenie dla kierownictwa
11. Szczegółowy zakres raportu zostanie ustalony na etapie zlecania prac, powyższe ma charakter zbioru zagadnień do wyboru. Raport należy dostarczyć Zamawiającemu w formie elektronicznej – w formacie .DOC i .PDF., najpóźniej w ostatnim dniu realizacji prac, audytu.

3.6. ZADANIE VI - RETESTY (PRAWO OPCJI)

1. Wykonawca zobowiązany jest do wykonania maksymalnie 6 tur retestów do zadań dotyczących audytu cyberbezpieczeństwa.
2. Zamawiający zleci wykonanie retestu w przypadku wdrożenia poprawek wynikających z raportu sporządzonego przez Wykonawcę po realizacji zadań dotyczących audytu cyberbezpieczeństwa.
4. Celem retestu jest weryfikacja usunięcia wykrytych podatności a także weryfikacja dokumentacji.
5. Do zadania VI zastosowanie ma procedura zlecania zadań lub części zadań opisana w rozdziale 3.7.2. OPZ.

3.7. ZLECANIE REALIZACJI ZADAŃ ZAMÓWIENIA

3.7.1. ZADANIA Z ZAKRESU ZAMÓWIENIA PODSTAWOWEGO

1. Zamawiający w trakcie obowiązywania umowy zleci realizację zadań z zakresu zamówienia podstawowego, tj. zadanie I oraz zadanie III.
2. Realizacja zadań zostanie zlecona przez osobę/-y uprawnione na podstawie umowy.

3. Zlecenie realizacji zadania zostanie podpisane przez osobę uprawnioną i wysłane na adres mailowy osoby uprawnionej po stronie Wykonawcy zgodnie z umową.
4. Zamawiający wskaże oczekiwany termin realizacji zadania, nie dłuższy niż 21 dni kalendarzowych.
5. Wykonawca przyjmie zlecenie realizacji zadania poprzez podpisanie wystawionego zlecenia. Wykonawca zobowiązany jest podpisać wystawione zlecenie w terminie nie dłuższym niż 2 dni robocze.
6. Termin realizacji zadania rozpoczyna bieg od momentu złożenia podpisu pod zleceniem przez Wykonawcę.
7. Przed przyjęciem zlecenia do realizacji zadania Wykonawca ma prawo do zażądania od Zamawiającego zorganizowania spotkania w celu doszczegółowienia zakresu obowiązków wynikających z zadania.
8. Po zakończeniu realizacji danego zadania, zostanie przeprowadzona procedura odbiorowa opisana w umowie.

3.7.2. ZADANIA Z ZAKRESU PRAWA OPCJI

1. Zamawiający do dnia zakończenia obowiązywania Umowy ma prawo, w ramach prawa opcji, zlecić realizację poszczególnych zadań zamówienia i retestów, zdefiniowanych jako prawo opcji.
2. Zamawiający skieruje do Wykonawcy w formie pisemnej lub elektronicznej z kwalifikowanym podpisem elektronicznym zlecenie realizacji danego zadania lub części zadania w ramach prawa opcji. Zlecenie to będzie zawierało co najmniej nazwę zadania oraz oczekiwany termin zakończenia realizacji, nie dłuższy niż 21 dni kalendarzowych.
3. Nie później niż w ciągu 3 dni roboczych Wykonawca potwierdzi w formie pisemnej lub elektronicznej z kwalifikowanym podpisem elektronicznym realizację zlecenia wykonania zadania lub części zadania lub przedstawi uwagi do zlecenia.
4. Zamawiający nie później niż w ciągu 2 dni roboczych przychyli się do kontrpropozycji Wykonawcy lub też odrzuci ją i podtrzyma pierwotną postać zlecenia. Wszelkie ustalenia, o których mowa w niniejszym ust. wymagają podpisu Stron.
5. Najpóźniej w ostatnim dniu terminu realizacji zadania lub części zadania, Wykonawca przedstawi Zamawiającemu w formie pisemnej lub elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym protokół odbioru wraz z raportem z realizacji zadania lub części zadania.

3.8. 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.

Infrastruktura badanego systemu znajduje się w Warszawie. 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.

4. HARMONOGRAM REALIZACYJNY

Zamawiający przewiduje, że wykonanie Zadania I odbędzie się w IV kw. 2024 r. Pozostałe zadania lub części zadań będą zlecane w zależności od potrzeb Zamawiającego, przy czym ich wykonanie musi się zakończyć w terminie obowiązywania umowy, tj. nie dłużej niż w ciągu 24 miesięcy od jej podpisania.

5. OPIS PLATFORMY SYSTEMOWEJ

5.1. CHARAKTERYSTYKA ROZWIĄZANIA - OPIS REALIZACJI TECHNICZNEJ ZAKRESU BIZNESOWEGO

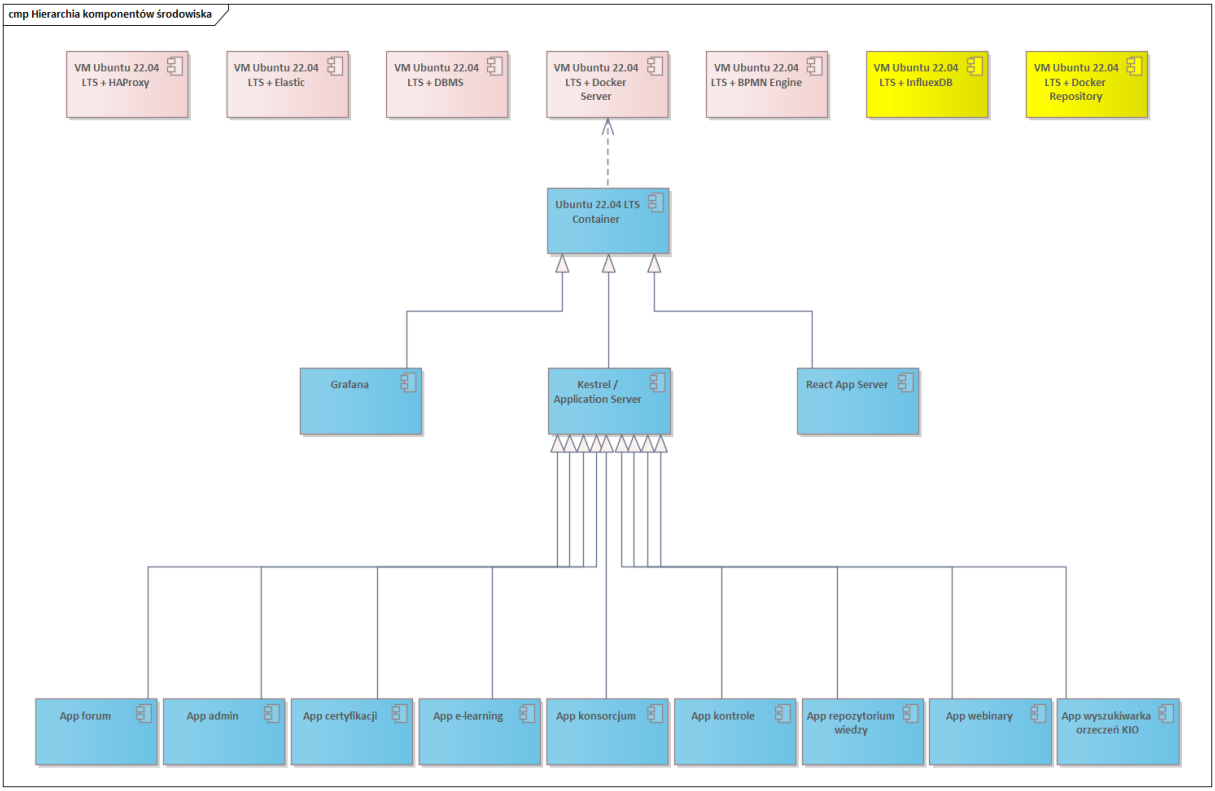
System PI PZ zostanie wytworzony z wykorzystaniem architektury trójwarstwowej. Aplikacja zrealizowana zostanie w postaci aplikacji internetowej dostępnej za pośrednictwem przeglądarki internetowej.

5.2. TECHNOLOGIE

System zostanie zaimplementowany w oparciu i z wykorzystaniem komponentów oprogramowania posiadających otwarte tryby licencjonowania (Open Source).
Na potrzeby wszystkich maszyn wirtualnych wykorzystanie zostanie system operacyjny Ubuntu 22.04 LTS.
Warstwa prezentacji (frontend) zrealizowana zostanie w postaci aplikacji internetowej w technologii React oraz Bootstrap. Warstwa logiki (backend) zrealizowana zostanie w postaci API w technologii .NET oraz języku C#. Warstwa danych (DB) zrealizowana zostanie w postaci relacyjnej bazy danych PostgreSQL oraz silnika wyszukiwania ElasticSearch. Za zarządzanie procesami biznesowymi odpowiadać będzie silnik procesowy Camunda Zeebe. Silnik ten będzie realizował procesy biznesowe zidentyfikowane w ramach prac analitycznych. Monitorowanie wewnętrzne zrealizowane zostanie za pośrednictwem oprogramowania Grafana i InfluxDB. Ruch sieciowy obsługiwany będzie przez HAProxy. Kontenery aplikacji obsługiwać będzie DockerServer. W celu wysyłki wiadomości z Systemu wykorzystany zostanie serwer pocztowy Postfix.

5.3. SKŁADOWE INFRASTRUKTURY ROZWIĄZANIA

W celu optymalizacji zasobów wszystkie serwery zarówno te podstawowe jak i zapasowy będą działać na równych zasadach – wszystkie będą równie obciążane i na każdym z serwerów będzie pewien zapas mocy pozwalający na przejście maszyn na wypadek awarii. Wszystkie serwery pracujące w ramach platformy będą połączone z macierzą dyskową, na której przetrzymywane będą wszystkie informacje związane z maszynami wirtualnymi dzięki czemu możliwe będzie migrowanie w locie maszyn między węzłami klastra wirtualizacyjnego. Do całego rozwiązania dostęp będzie chroniony na poziomie sieciowym dzięki zastosowaniu urządzenia UTM lub WAF, na takim urządzeniu będzie też terminowany ruch SSL.
Poniższy schemat przedstawia ogólny zakres bez podziału na poszczególne środowiska jest on przekrojem przykładowym.



Rysunek 1 Schemat hierarchii komponentów środowiska

Na przedstawionym schemacie widoczne są dwa główne poziomy czyli poziom serwerów z zainstalowanym oprogramowaniem narzędziowym oraz poziom konteneryzacji, który to jest rozszerzalny do poszczególnych kontenerów zadaniowych. Widoczny na schemacie trzeci poziom jest poziomem głównym kontenerów, widać tu trzy główne rodzaje kontenerów, z których każdy generalizuje pewne funkcjonalności – Grafana (komponent służący do analizy), React App (komponent wizualizacji systemu), Kestrel (komponenty odpowiadające za obsługę wszystkich modułów pod względem dostarczania danych). Na samym dole schematu mamy rozpisane wszystkie aplikacje funkcjonalne, które są rzeczywistości modułami API serwującymi dane do poszczególnych części systemu. Na powyższym schemacie widać też zróżnicowanie na poziomie serwerów – pierwsza część widoczna od lewej strony to grupy serwerów wyspecyfikowane pod konkretne środowisko, w drugiej części widocznej od prawej czyli na schemacie oznaczone żółtym kolorem są to serwery globalne, które będą jednoinstancyjne i dostępne z wszystkich środowisk.

5.4. ARCHITEKTURA ROZWIĄZANIA

5.4.1. OGÓLNY OPIS ARCHITEKTURY ROZWIĄZANIA – PODZIAŁ SYSTEMU NA MODUŁY FUNKCJONALNE

System jest zbudowany zgodnie z SOA (Service Oriented Architecture) w oparciu o niezależne moduły, z których każdy realizuje zestaw określonych funkcji i jest udostępniany użytkownikom jako usługa.
Moduł administracyjny jest dostępny z wyznaczonych lokalizacji, nie ma do niego publicznego dostępu. Pozostałe moduły są dostępne publicznie.

Rozwiązanie składa się z następujących głównych komponentów:

1. PI_PZ.App
2. PI_PZ.Admin.API
3. PI_PZ.Base.API
4. PI_PZ.Consortium.API
5. PI_PZ.Forum.API
6. PI_PZ.Inspection.API
7. PI_PZ.Knowledge.API

8. PI_PZ.Service

5.4.1.1. PI_PZ.APP

Aplikacja odpowiadająca za warstwę prezentacji zrealizowana w postaci aplikacji internetowej w technologii React oraz Bootstrap. Interfejs aplikacji generowany do postaci stron WWW obsługiwanych przez popularne przeglądarki internetowe – Chrome, Firefox, Edge, Safari.
Aplikacja korzystaz API modułów wchodzących w skład Systemu PI PZ.
Zarządzanie stanem w aplikacji React zrealizowane jest poprzez Context API.

5.4.1.2. API

API zwraca dane w postaci JSON oraz stosowne kody odpowiedzi http.

5.4.1.2.1. PI_PZ.ADMIN.API

Internetowy interfejs API odpowiadający za realizację logiki biznesowej modułu administracyjnego Systemu PI PZ. Komunikuje się z warstwą danych.

5.4.1.2.2. PI_PZ.BASE.API

Internetowy interfejs API odpowiadający za realizację logiki biznesowej części wspólnych Systemu PI PZ. komunikuje się z warstwą danych.PI_PZ.Consortium.API.
Internetowy interfejs API odpowiadający za realizację logiki biznesowej modułu konsorcjum Systemu PI PZP. komunikuje się będzie z warstwą danych.

5.4.1.2.3. PI_PZ.FORUM.API

Internetowy interfejs API odpowiadający za realizację logiki biznesowej modułu forum Systemu PI PZ. komunikuje się z warstwą danych.

5.4.1.2.4. PI_PZ.INSPECTION.API

Internetowy interfejs API odpowiadający za realizację logiki biznesowej modułu kontroli Systemu PI PZ. komunikuje się z warstwą danych.

5.4.1.2.5. PI_PZ.KNOWLEDGE.API

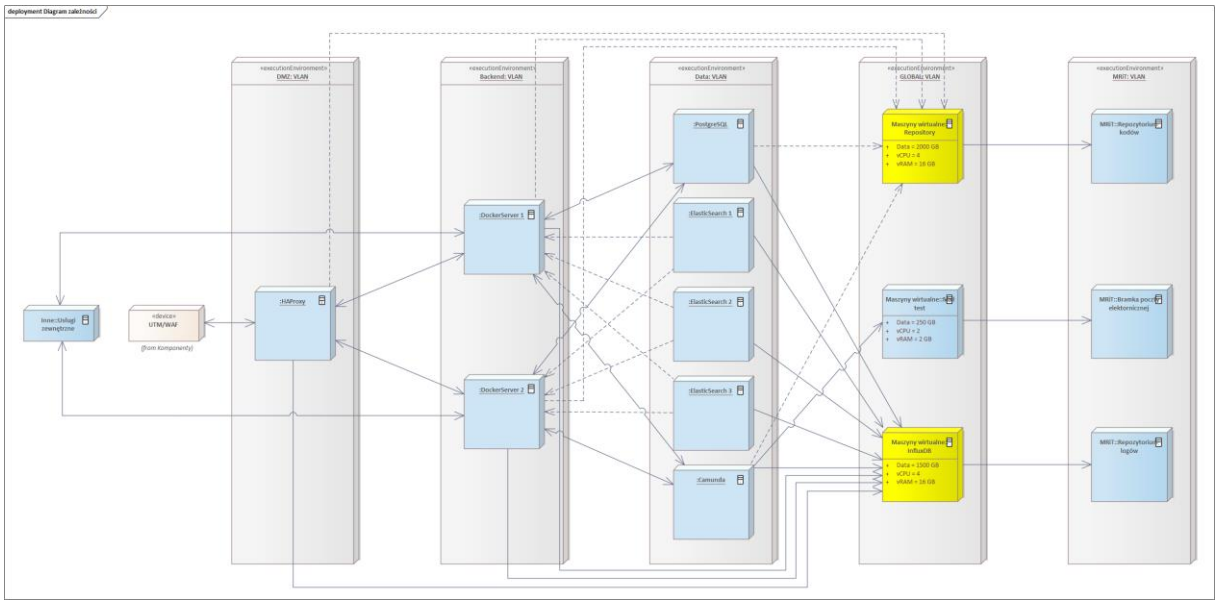
Internetowy interfejs API odpowiadający za realizację logiki biznesowej modułu repozytorium wiedzy Systemu PI PZ. komunikuje się będzie z warstwą danych.

5.4.1.2.6. PI_PZ.SERVICE

Usługa odpowiadająca za wykonywanie cyklicznych operacji takich jak wysyłka wiadomości e-mail, archiwizacja powiadomień komunikuje się z warstwą danych.

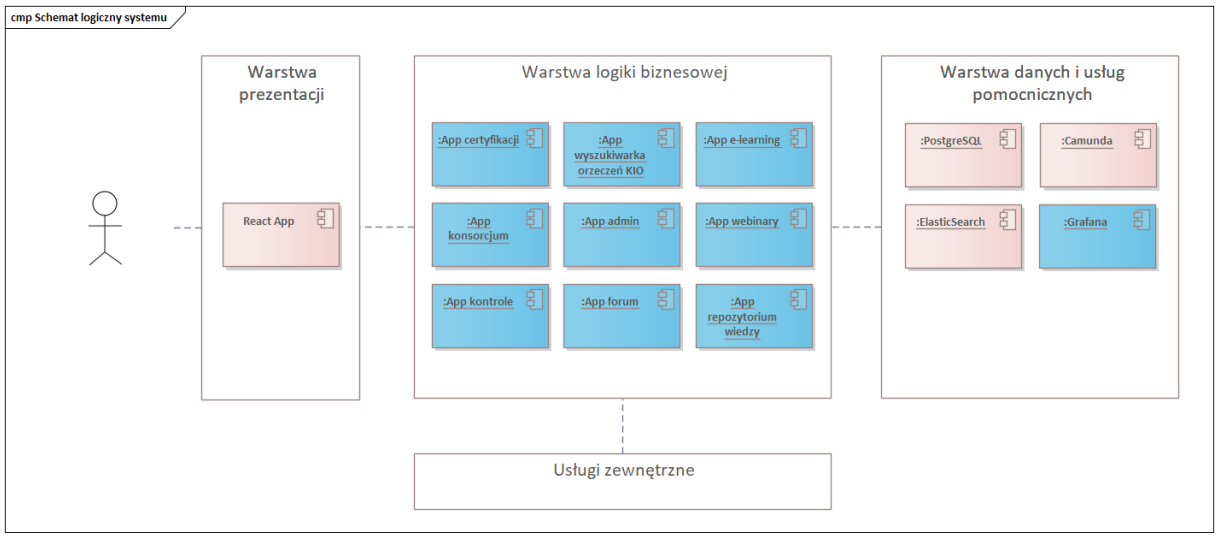
5.4.2. ARCHITEKTURA SYSTEMU

System PI PZ został wytworzony z wykorzystaniem architektury trójwarstwowej. Architektura Systemu PI PZ wraz z przepływami danych pomiędzy modułami oraz połączeniami z zewnętrznymi komponentami została przedstawiona na poniższym rysunku.



Rysunek 2 Ogólny diagram zależności systemu

Architektura trójwarstwowa jest zorganizowana w oparciu o następujące warstwy – w warstwie prezentacji jest to aplikacja w technologii React, która jest uruchamiana w przeglądarce internetowej użytkownika. Warstwa prezentacji komunikuje się z warstwą logiki biznesowej realizowanej przez moduły REST API zrealizowane w postaci aplikacji opartej o Kestrel i zamkniętej w postaci kontenerów na serwerach aplikacyjnych oznaczonych jako DockerServer. Warstwa logiki działa w oparciu o dane zlokalizowane w warstwie danych, które to zlokalizowane są na serwerach bazodanowych realizowanych przez PostgreSQL oraz ElasticSearch.



Rysunek 3 Schemat logiczny systemu

5.4.3. ARCHITEKTURA BEZPIECZEŃSTWA SYSTEMU

W zakresie bezpieczeństwa system PI PZ jest zbudowany w oparciu o podział rozwiązania na warstwy w tym warstwę prezentacyjna, logiczną oraz danych. Oprócz podziału rozwiązania na warstwy logiczne rozwiązanie jest podzielone również na strefy bezpieczeństwa sieciowe VLAN. Podział sieci na VLAN to podział sieci fizycznej na sieci logiczne, które pozwala na odseparowanie określonych stref od siebie i umożliwienie ruchu między strefami na wskazanych portach /

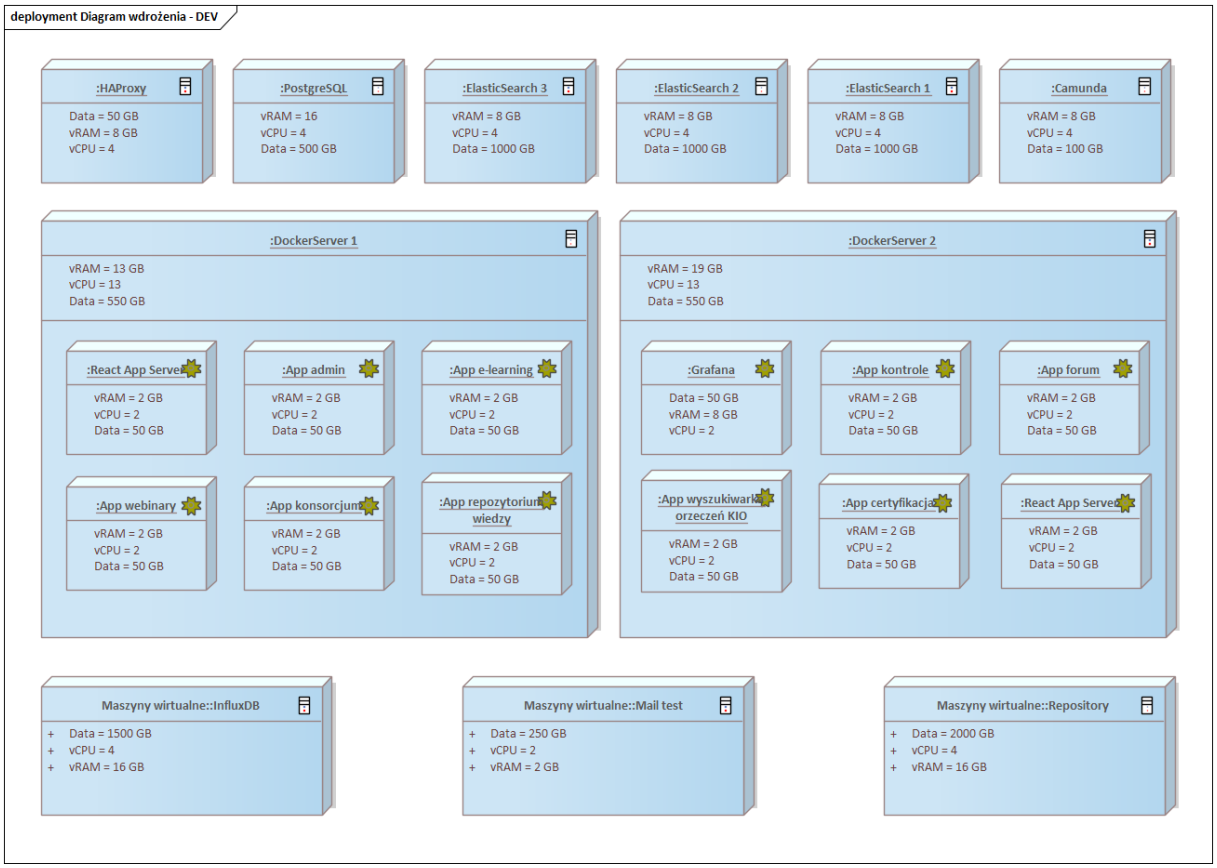
protokołach. Urządzenie brzegowe terminuje ruch SSL – to na tym urządzeniu są zainstalowane certyfikaty SSL i ruch do tego urządzenia odbywa się z wykorzystaniem protokołu HTTPS. Wewnątrz sieci Ministerstwa – za urządzeniami brzegowymi ruch odbywa się już bez szyfrowania co pozwalana na optymalizację mocy obliczeniowej potrzebnej przez poszczególne warstwy na terminowanie SSL.
W warstwie aplikacyjnej za zabezpieczenie odpowiada system tokenów – podczas logowania użytkownika oraz cyklicznie podczas jego pracy w systemie są generowane tokeny, dzięki którym żądania użytkownika wysyłane z przeglądarki do modułów funkcjonalnych API są zautoryzowane.

5.4.4. STANDARDY INTEGRACYJNE I METODY KOMUNIKACJI

System zintegrowany jest z Systemami zewnętrznymi takimi jak: Węzeł Krajowy, API BZP, API UZP, API TED, eKONTROLE, Hurtownia Danych CEIDG. Komunikacja na stykach integracyjnych jest w pełni szyfrowana, całość transmisji pomiędzy Systemami odbywa się w szyfrowanym kanale komunikacyjnym SSL. Rozwiązanie takie zapewnia wysokie bezpieczeństwo dostarczanych usług oraz przetwarzanych danych, w tym danych osobowych i wrażliwych.
Komunikacja odbywa się za pośrednictwem API lub za pośrednictwem żądań HTTP-POST. Model wdrożenia:
Platforma została wdrożona w pięciu środowiskach o następującym przeznaczeniu:

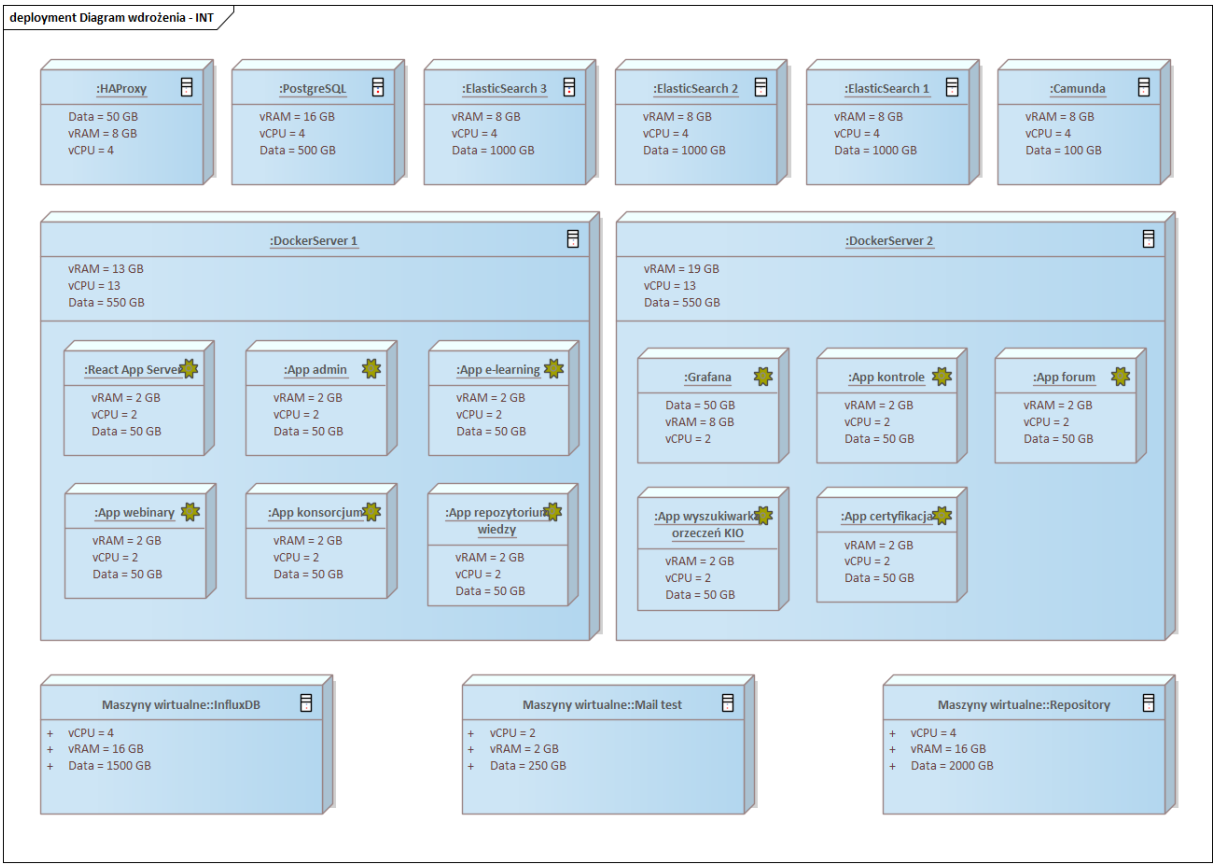
- DEV – środowisko przeznaczone do rozwoju systemu,
- INT – środowisko do integracji komponentów systemu oraz do wstępnych testów integracji,
- TEST – środowisko testowe, służące głównie do weryfikacji systemu od strony funkcjonalnej oraz użytkowej,
- PRE-PROD – środowisko umożliwiające weryfikację realnych przypadków użycia systemu (z wykorzystaniem danych produkcyjnych) oraz służące do badania wydajności systemu,
- PROD – produkcyjne środowisko systemu.

Środowiska zostały wyskalowane pod kątem przydziału zasobów w sposób adekwatny do ich przeznaczenia. Środowisko DEV ma zasoby wystarczające do rozwoju systemu. W szczególności system posiada wszystkie komponenty funkcjonalne. Zasoby zostały przydzielone zgodnie z opisami na poniższym diagramem.



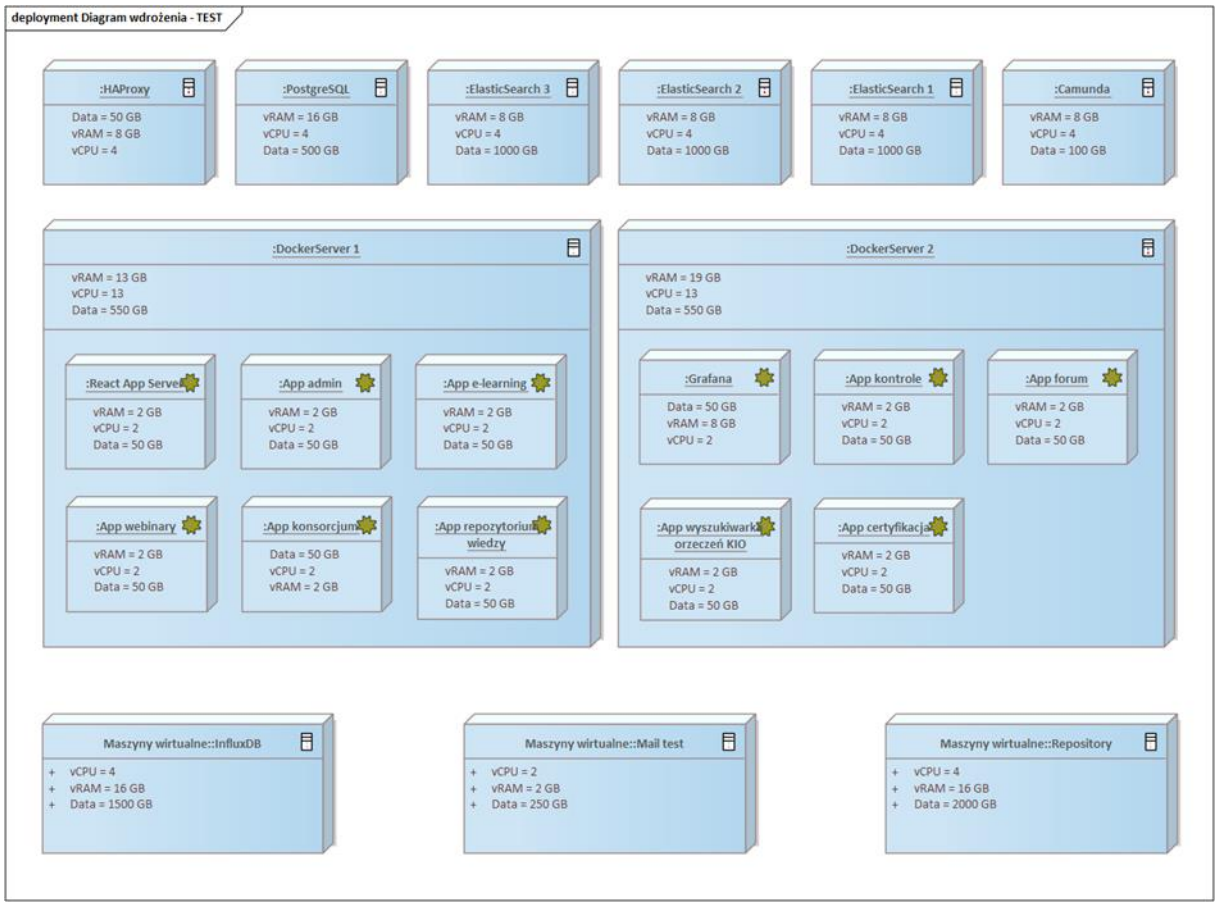
Rysunek 4 Diagram wdrożenia środowiska deweloperskiego (DEV)

Środowisko integracyjne będzie ma analogiczny przydział zasobów, który wystarczy do weryfikacji poprawnej integracji wszystkich komponentów składowych systemu. Szczegóły alokacji fizycznych zasobów obrazuje poniższy rysunek.



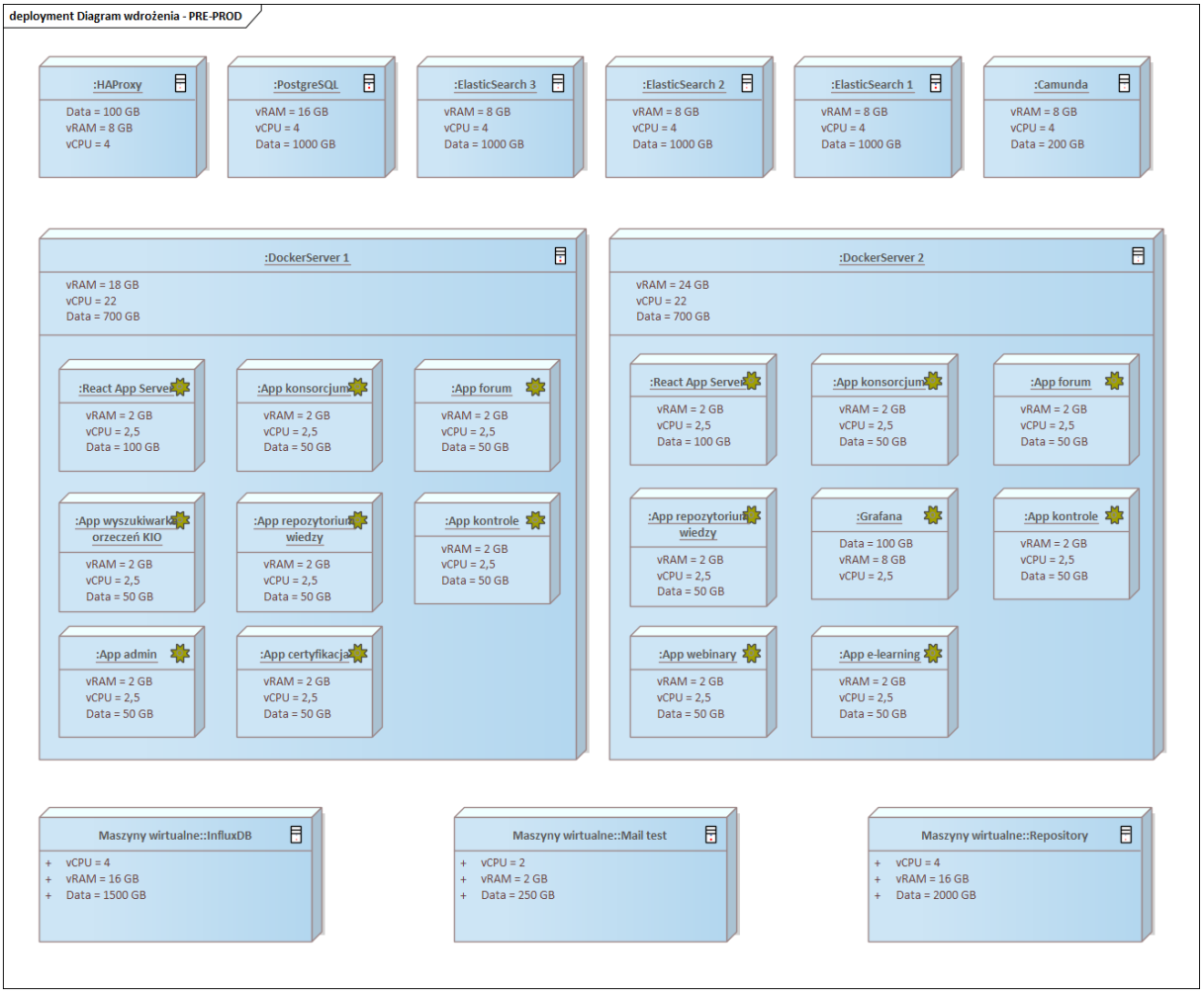
Rysunek 5 Diagram wdrożenia środowiska integracyjnego (INT)

Również środowisko testowe posiada analogiczny przydział zasobów. Różni się od poprzednich środowisk tym, iż (w miarę możliwości i dostępności) jest połączone z testowymi instancjami usług zewnętrznych dostawców.



Rysunek 6 Diagram wdrożenia środowiska testowego (TEST)

Środowisko PRE-PROD dysponuje zasobami analogicznymi do środowiska produkcyjnego. Ma to w zamyśle zapewnić odtworzenie produkcyjnych danych w celu zweryfikowania zachowania systemu w realnych przypadkach. W związku z tym przydział pojemności dyskowych oraz wydajność tych zasobów jest identyczna, jak w środowisku produkcyjnym. Co więcej, w celu umożliwienia poprawnego wykonania testów wydajności, analogiczne do środowiska są zasoby wpływające na ogólną wydajność środowiska, tj. przydział pamięci oraz procesorów logicznych. Z uwagi na konieczność zachowania bezpieczeństwa przetwarzania danych produkcyjnych, środowisko PRE-PROD nie posiada możliwości wysyłania jakichkolwiek informacji na zewnątrz (poza ściśle kontrolowanymi przypadkami).
Szczegółowy plan przydziału zasobów fizycznych platformy PRE-PROD obrazuje niżej zamieszczony diagram.

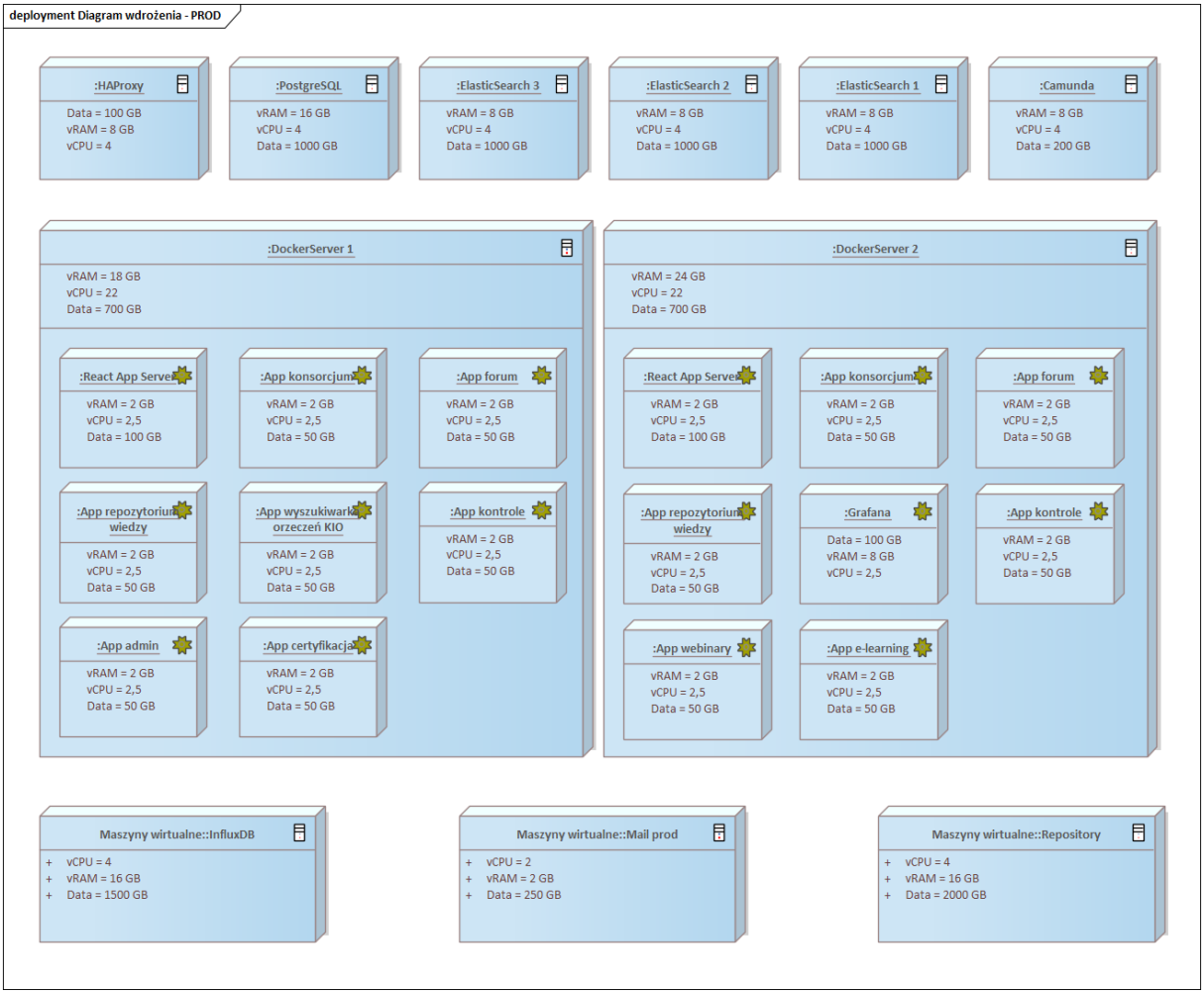


Rysunek 7 Diagram wdrożenia środowiska przedprodukcyjnego (PRE-PROD)

Środowisko produkcyjne jest uruchomione w oparciu o węzły dysponujące zasobami jak na poniższym rysunku. Konfiguracja środowiska jest skonstruowana w sposób umożliwiający swobodne skalowanie poziome rozwiązania, tj. możliwe będzie powielanie poszczególnych węzłów funkcjonalnych w celu zwiększenia wydajności w wydzielonym obszarze.

Środowisko produkcyjne jest uruchomione w oparciu o maszyny zwirtualizowane w tradycyjny sposób oraz częściowo w formule konteneryzacji. Środowisko wirtualizacyjne zapewnia mechanizmy gwarantujące wysoką dostępność (ang. High Availability) kluczowych elementów platformy. Zasoby dyskowe zostały wyskalowane w sposób umożliwiający niezawodne działanie systemu przez co najmniej 5 lat przy założeniu braku znaczącego wzrostu zapotrzebowania na przestrzeń.

Zamieszczony niżej diagram szczegółowo obrazuje rozmieszczenie komponentów na węzłach fizycznych oraz planowany przydział zasobów.



Rysunek 8 Diagram wdrożenia środowiska produkcyjnego (PROD)

5.4.5. INFRASTRUKTURA FIZYCZNA I WIRTUALNA

Składowe infrastruktury rozwiązania cała infrastruktura fizyczna składa się z 5 identycznych serwerów, z których cztery pełnią funkcję podstawowych serwerów a piąty serwer jest serwerem zapasowym. Aby zoptymalizować zasoby oraz wykorzystanie tych zasobów, wszystkie serwery są wykorzystywane w równej mierze co oznacza że każdy z serwerów zawiera prawie identyczną listę maszyn wirtualnych jednak są one zróżnicowane pod kątem środowiska – każdy fizyczny serwer zawiera na przykład maszyny wirtualne odpowiadające za obsługę ruchu czyli HAProxy jednak na każdym z serwerów jest ona przynależna do innego środowiska. Podział środowisk rotuje w zakresie maszyn dzięki czemu rozłożony zostanie ruch środowiska produkcyjnego na różne węzły klastra a tym samym zwiększy to wydajność środowiska. Na poniższym diagramie przedstawiony został rozkład maszyn wirtualnych na poszczególnych serwerach fizycznych.

Rysunek 9 Diagram infrastruktury fizycznej

Każda maszyna ma zaproponowane parametry podstawowe, które są rekomendacją w zakresie wymaganej infrastruktury sprzętowej dedykowanej do realizacji zadań projektowanego systemu. Rekomendacje zostały zebrane w postaci poniższej tabeli.

Tabela 1 Sugerowane parametry serwerów fizycznych

Nazwa serwera	CPU	RAM (GB)	HDD (GB)
Serwer 1	2 x 16 HT	196	2 x 300
Serwer 2	2 x 16 HT	196	2 x 300
Serwer 3	2 x 16 HT	196	2 x 300
Serwer 4	2 x 16 HT	196	2 x 300
Serwer 5	2 x 16 HT	196	2 x 300

Pod kątem wydajnościowym zalecane serwery wyposażone w procesory wykazujące w testach „cpubenchmark" minimalny wynik w zakresie „Thread Mark" o wartości 2553.
Oprócz opisanej wyżej rekomendacji w zakresie infrastruktury serwerowej ważnym aspektem jest przestrzeń dyskowa podłączona do wszystkich wyżej wymienionych serwerów fizycznych – macierz dyskowa. W zakresie macierzy dyskowej wymagane jest aby dostarczyć przestrzeń dyskową o minimalnej objętości 30TB do wykorzystania co oznacza, że w przypadku zastosowania na przykład RAID6 oraz dysków SSD o pojemności na przykład 7TB należy zastosować co najmniej 7 dysków które finalnie dadzą do wykorzystania około 32TB przestrzeni i dopuszczą awarię 2 dysków.
W warstwie wirtualizacji każdy z serwerów fizycznych będzie posiadał zbliżone ilości maszyn wirtualnych o zbliżonym sumarycznym zapotrzebowaniu na pamięć oraz procesory. Każde ze środowisk będzie zawierało analogiczny skład maszyn wirtualnych, które jednak będą zróżnicowane pod kątem zasobów w zależności od środowiska, na które zostały zaprojektowane. W poniższych podrozdziałach znajduje się rozkład maszyn wirtualnych oraz ich zawartość w podziale na środowiska. W każdym środowisku obecne są 3 maszyny wirtualne które wchodzą w skład grupy maszyn globalnych – są to maszyny, które muszą wchodzić w skład każdego środowiska i zbierają dane z wszystkich lub części środowisk.
Poniżej znajduje się ogólny rozkład maszyn wirtualnych na proponowanych serwerach fizycznych obrazujący margines bezpieczeństwa pozostający na serwerach.

Tabela 2 Alokacja zasobów na serwerach fizycznych przez maszyny wirtualne

Nazwa serwera	Liczba VM	CPU logiczne	vCPU	RAM (GB)	vRAM (GB)
Serwer 1	8	64	68	196	98
Serwer 2	9	64	61	196	95
Serwer 3	9	64	54	196	104
Serwer 4	9	64	54	196	104
Serwer 5	9	64	61	196	95

3.4.1.1. ŚRODOWISKO DEWELOPERSKIE (DEV)

Środowisko deweloperskie będzie służyło do wstępnych testów wersji rozwojowych oprogramowania, w skład środowiska wchodzić będą maszyny odpowiedzialne z dystrybucję ruchu (HAProxy), składowanie danych biznesowych (PosrgreSQL), składowanie danych wyszukiwawczych (ElasticSearch), zarządzanie procesami biznesowymi (Camunda), konteneryzacje (DockerServer). Dodatkowo obecne tu będą 3 serwery globalne w skład których wejdzie serwer danych analitycznych (InfluxDB), serwer repozytorium kodów i obrazów (Repository) oraz serwer pocztowy testowy (Mail test). Rysunek 4 Diagram wdrożenia środowiska deweloperskiego (DEV) prezentuje wszystkie wymienione maszyny oraz posadowione na nich kontenery w przypadku serwerów konteneryzacji. Poniżej znajduje się zestawienie parametrów maszyn wirtualnych przewidzianych na środowisko deweloperskie, które zawiera podstawowe informacje takie jak objętość dysków, zapotrzebowanie na ram oraz wirtualne rdzenie procesora.

Tabela 3 Parametry maszyn wirtualnych środowiska deweloperskiego

Nazwa maszyny wirtualnej	vCPU	vRAM (GB)	HDD (GB)
HAProxy	4	8	50
PostgreSQL	4	16	500

ElasticSearch 1	4	8	1000
ElasticSearch 2	4	8	1000
ElasticSearch 3	4	8	1000
Camunda	4	8	100
DockerServer 1	13	13	550
DockerServer 2	13	19	550

W ramach środowiska na serwerach konteneryzacji zostaną wdrożone obrazy kontenerów które w większości będą wytarzane w procesie ciągłej integracji zmian w kodzie ciągłego wdrażania (CI/CD). Jedyny kontener, który nie będzie objęty procesem CI/CD to kontener zawierający oprogramowanie Grafana – w tym przypadku wdrożone zostanie najaktualniejsze oficjalne wydanie wskazanego oprogramowania z uwagi na fakt iż zostanie tu użyte gotowe oprogramowanie. Wszystkie pozostałe kontenery będą zbudowane w oparciu o wymieniony wyżej proces i zawierać będą dedykowane rozwiązania realizujące funkcjonalnie zadania, do których zostały stworzone. Poniżej znajduje się wykaz kontenerów, które będą dostarczone w ramach środowiska deweloperskiego, w wykazie ujęte zostały kontenery na potrzeby modułów, które są objęte prawem opcji czyli ich wdrożenie uzależnione jest od decyzji zlecenia.

Tabela 4 Parametry kontenerów na środowisku deweloperskim

Nazwa kontenera	vCPU	vRAM (GB)	HDD (GB)	Opis
React App Server	2	2	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
App admin	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu administracyjnego przez API
App e-learning	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu e-learning przez API. Moduł opcjonalny.
App webinary	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu webinary przez API. Moduł opcjonalny.
App konsorcjum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App repozytorium wiedzy	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
Grafana	2	8	50	Kontener odpowiedzialny za obsługę monitorowania systemu we wszystkich aspektach.
App kontrole	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App forum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.
App wyszukiwarka orzeczeń KIO	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu wyszukiwarki orzeczeń KIO przez API.
App certyfikacja	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu certyfikacji przez API. Moduł opcjonalny.
React App Server	2	2	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT.

5.4.5.1. ŚRODOWISKO INTEGRACYJNE (INT)

Środowisko integracyjne będzie służyło do testów integracji modułów oprogramowania, w skład środowiska wchodzić będą maszyny odpowiedzialne z dystrybucję ruchu (HAProxy), składowanie danych biznesowych (PosrgreSQL),

składowanie danych wyszukiwawczych (ElasticSearch), zarządzanie procesami biznesowymi (Camunda), konteneryzacje (DockerServer). Dodatkowo obecne tu będą 3 serwery globalne w skład których wejdzie serwer danych analitycznych (InfluxDB), serwer repozytorium kodów i obrazów (Repository) oraz serwer pocztowy testowy (Mail test). Rysunek 5 Diagram wdrożenia środowiska integracyjnego (INT) prezentuje wszystkie wymienione maszyny oraz posadowione na nich kontenery w przypadku serwerów konteneryzacji. Poniżej znajduje się zestawienie parametrów maszyn wirtualnych przewidzianych na środowisko integracyjne, które zawiera podstawowe informacje takie jak objętość dysków, zapotrzebowanie na ram oraz wirtualne rdzenie procesora.

Tabela 5 Parametry maszyn wirtualnych środowiska integracyjnego

Nazwa maszyny wirtualnej	vCPU	vRAM (GB)	HDD (GB)
HAProxy	4	8	50
PostgreSQL	4	16	500
ElasticSearch 1	4	8	1000
ElasticSearch 2	4	8	1000
ElasticSearch 3	4	8	1000
Camunda	4	8	100
DockerServer 1	13	13	550
DockerServer 2	13	19	550

W ramach środowiska na serwerach konteneryzacji zostaną wdrożone obrazy kontenerów, które w większości będą wytarzane w procesie ciągłej integracji zmian w kodzie ciągłego wdrażania (CI/CD). Jedyny kontener, który nie będzie objęty procesem CI/CD to kontener zawierający oprogramowania Grafana – w tym przypadku wdrożone zostanie najaktualniejsze oficjalne wydanie wskazanego oprogramowania z uwagi na fakt iż zostanie tu użyte gotowe oprogramowanie. Wszystkie pozostałe kontenery będą zbudowane w oparciu o wymieniony wyżej proces i zawierać będą dedykowane rozwiązania realizujące funkcjonalnie zadania do których zostały stworzone. Poniżej znajduje się wykaz kontenerów, które będą dostarczone w ramach środowiska integracyjnego, w wykazie ujęte zostały kontenery na potrzeby modułów, które są objęte prawem opcji czyli ich wdrożenie uzależnione jest od decyzji zlecenia.

Tabela 6 Parametry kontenerów na środowisku integracyjnym

Nazwa kontenera	vCPU	vRAM (GB)	HDD (GB)	Opis
React App Server	2	2	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
App admin	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu administracyjnego przez API
App e-learning	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu e-learning przez API. Moduł opcjonalny.
App webinary	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu webinary przez API. Moduł opcjonalny.
App konsorcjum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App repozytorium wiedzy	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
Grafana	2	8	50	Kontener odpowiedzialny za obsługę monitorowania systemu we wszystkich aspektach.
App kontrole	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App forum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.

App wyszukiwarka orzeczeń KIO	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu wyszukiwarki orzeczeń KIO przez API.
App certyfikacja	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu certyfikacji przez API. Moduł opcjonalny.

5.4.5.2. ŚRODOWISKO TESTOWE (TEST)

Środowisko testowe będzie służyło do testów funkcjonalnych oprogramowania, będzie tu też można przeprowadzać wstępne testy wydajnościowe oraz bezpieczeństwa. W skład środowiska wchodzić będą maszyny odpowiedzialne z dystrybucję ruchu (HAProxy), składowanie danych biznesowych (PosrgreSQL), składowanie danych wyszukiwawczych (ElasticSearch), zarządzanie procesami biznesowymi (Camunda), konteneryzacje (DockerServer). Dodatkowo obecne tu będą 3 serwery globalne w skład których wejdzie serwer danych analitycznych (InfluxDB), serwer repozytorium kodów i obrazów (Repository) oraz serwer pocztowy testowy (Mail test). Rysunek 6 Diagram wdrożenia środowiska testowego (TEST) prezentuje wszystkie wymienione maszyny oraz posadowione na nich kontenery w przypadku serwerów konteneryzacji. Poniżej znajduje się zestawienie parametrów maszyn wirtualnych przewidzianych na środowisko testowe, które zawiera podstawowe informacje takie jak objętość dysków, zapotrzebowanie na ram oraz wirtualne rdzenie procesora.

Tabela 7 Parametry maszyn wirtualnych środowiska testowego

Nazwa maszyny wirtualnej	vCPU	vRAM (GB)	HDD (GB)
HAProxy	4	8	50
PostgreSQL	4	16	500
ElasticSearch 1	4	8	1000
ElasticSearch 2	4	8	1000
ElasticSearch 3	4	8	1000
Camunda	4	8	100
DockerServer 1	13	13	550
DockerServer 2	13	19	550

W ramach środowiska na serwerach konteneryzacji zostaną wdrożone obrazy kontenerów, które w większości będą wytarzane w procesie ciągłej integracji zmian w kodzie ciągłego wdrażania (CI/CD). Jedyny kontener, który nie będzie objęty procesem CI/CD to kontener zawierający oprogramowania Grafana – w tym przypadku wdrożone zostanie najaktualniejsze oficjalne wydanie wskazanego oprogramowania z uwagi na fakt iż zostanie tu użyte gotowe oprogramowanie. Wszystkie pozostałe kontenery będą zbudowane w oparciu o wymieniony wyżej proces i zawierać będą dedykowane rozwiązania realizujące funkcjonalnie zadania, do których zostały stworzone. Poniżej znajduje się wykaz kontenerów, które będą dostarczone w ramach środowiska testowego, w wykazie ujęte zostały kontenery na potrzeby modułów które są objęte prawem opcji czyli ich wdrożenie uzależnione jest od decyzji zlecenia.

Tabela 8 Parametry kontenerów na środowisku testowym

Nazwa kontenera	vCPU	vRAM (GB)	HDD (GB)	Opis
React App Server	2	2	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
App admin	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu administracyjnego przez API
App e-learning	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu e-learning przez API. Moduł opcjonalny.
App webinary	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu webinary przez API. Moduł opcjonalny.

App konsorcjum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App repozytorium wiedzy	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
Grafana	2	8	50	Kontener odpowiedzialny za obsługę monitorowania systemu we wszystkich aspektach.
App kontrole	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App forum	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.
App wyszukiwarka orzeczeń KIO	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu wyszukiwarki orzeczeń KIO przez API.
App certyfikacja	2	2	50	Kontener odpowiedzialny za serwowanie danych do modułu certyfikacji przez API. Moduł opcjonalny.

5.4.5.3. ŚRODOWISKO PRZEDPRODUKCYJNE (PRE-PROD)

Środowisko przedprodukcyjne będzie służyło do testów funkcjonalności oprogramowania na danych produkcyjnych bez funkcjonalności, które wymagają dostępu do zintegrowanych systemów obcych, możliwe tu również będzie przeprowadzanie testów wydajnościowych. W skład środowiska wchodzić będą maszyny odpowiedzialne z dystrybucję ruchu (HAProxy), składowanie danych biznesowych (PosrgreSQL), składowanie danych wyszukiwawczych (ElasticSearch), zarządzanie procesami biznesowymi (Camunda), konteneryzacje (DockerServer). Dodatkowo obecne tu będą 3 serwery globalne w skład których wejdzie serwer danych analitycznych (InfluxDB), serwer repozytorium kodów i obrazów (Repository) oraz serwer pocztowy testowy (Mail test). Rysunek 7 Diagram wdrożenia środowiska przedprodukcyjnego (PRE-PROD) prezentuje wszystkie wymienione maszyny oraz posadowione na nich kontenery w przypadku serwerów konteneryzacji. Poniżej znajduje się zestawienie parametrów maszyn wirtualnych przewidzianych na środowisko przedprodukcyjne, które zawiera podstawowe informacje takie jak objętość dysków, zapotrzebowanie na ram oraz wirtualne rdzenie procesora.

Tabela 9 Parametry maszyn wirtualnych środowiska przedprodukcyjnego

Nazwa maszyny wirtualnej	vCPU	vRAM (GB)	HDD (GB)
HAProxy	4	8	100
PostgreSQL	4	16	1000
ElasticSearch 1	4	8	1000
ElasticSearch 2	4	8	1000
ElasticSearch 3	4	8	1000
Camunda	4	8	200
DockerServer 1	22	18	700
DockerServer 2	22	24	700

W ramach środowiska na serwerach konteneryzacji zostaną wdrożone obrazy kontenerów, które w większości będą wytarzane w procesie ciągłej integracji zmian w kodzie ciągłego wdrażania (CI/CD). Jedyny kontener, który nie będzie objęty procesem CI/CD to kontener zawierający oprogramowania Grafana – w tym przypadku wdrożone zostanie najaktualniejsze oficjalne wydanie wskazanego oprogramowania z uwagi na fakt iż zostanie tu użyte gotowe oprogramowanie. Wszystkie pozostałe kontenery będą zbudowane w oparciu o wymieniony wyżej proces i zawierać będą dedykowane rozwiązania realizujące funkcjonalnie zadania do których zostały stworzone. Poniżej znajduje się wykaz kontenerów, które będą dostarczone w ramach środowiska przedprodukcyjnego, w wykazie ujęte zostały kontenery na potrzeby modułów które są objęte prawem opcji czyli ich wdrożenie uzależnione jest od decyzji zlecenia.

Tabela 10 Parametry kontenerów na środowisku przedprodukcyjnym

Nazwa kontenera	vCPU	vRAM (GB)	HDD (GB)	Opis
React App Server	2	2,5	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
React App Server	2	2,5	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
App admin	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu administracyjnego przez API
App e-learning	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu e-learning przez API. Moduł opcjonalny.
App webinary	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu webinary przez API. Moduł opcjonalny.
App konsorcjum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App konsorcjum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App repozytorium wiedzy	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
App repozytorium wiedzy	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
Grafana	2	8	50	Kontener odpowiedzialny za obsługę monitorowania systemu we wszystkich aspektach.
App kontrole	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App kontrole	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App forum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.
App forum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.
App wyszukiwarka orzeczeń KIO	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu wyszukiwarki orzeczeń KIO przez API.
App certyfikacja	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu certyfikacji przez API. Moduł opcjonalny.

5.4.5.4. ŚRODOWISKO PRODUKCYJNE (PROD)

Środowisko produkcyjne będzie służyło do obsługi ruchu produkcyjnego (eksploatacji produkcyjnej), na tym środowisku nie będą przeprowadzane żadne testy. W skład środowiska wchodzić będą maszyny odpowiedzialne z dystrybucję ruchu (HAProxy), składowanie danych biznesowych (PosrgreSQL), składowanie danych wyszukiwawczych (ElasticSearch), zarządzanie procesami biznesowymi (Camunda), konteneryzacje (DockerServer). Dodatkowo obecne tu będą 3 serwery globalne w skład których wejdzie serwer danych analitycznych (InfluxDB), serwer repozytorium kodów i obrazów (Repository) oraz serwer pocztowy produkcyjny (Mail prod). Rysunek 8 Diagram wdrożenia środowiska produkcyjnego (PROD) prezentuje wszystkie wymienione maszyny oraz posadowione na nich kontenery w przypadku serwerów konteneryzacji. Poniżej znajduje się zestawienie parametrów maszyn wirtualnych przewidzianych na środowisko produkcyjne, które zawiera podstawowe informacje takie jak objętość dysków, zapotrzebowanie na ram oraz wirtualne rdzenie procesora.

Tabela 11 Parametry maszyn wirtualnych środowiska produkcyjnego

Nazwa maszyny wirtualnej	vCPU	vRAM (GB)	HDD (GB)
HAProxy	4	8	100
PostgreSQL	4	16	1000
ElasticSearch 1	4	8	1000
ElasticSearch 2	4	8	1000
ElasticSearch 3	4	8	1000
Camunda	4	8	200
DockerServer 1	22	18	700
DockerServer 2	22	24	700

W ramach środowiska na serwerach konteneryzacji zostaną wdrożone obrazy kontenerów, które w większości będą wytarzane w procesie ciągłej integracji zmian w kodzie ciągłego wdrażania (CI/CD). Jedyny kontener który nie będzie objęty procesem CI/CD to kontener zawierający oprogramowania Grafana – w tym przypadku wdrożone zostanie najaktualniejsze oficjalne wydanie wskazanego oprogramowania z uwagi na fakt iż zostanie tu użyte gotowe oprogramowanie. Wszystkie pozostałe kontenery będą zbudowane w oparciu o wymieniony wyżej proces i zawierać będą dedykowane rozwiązania realizujące funkcjonalnie zadania, do których zostały stworzone. Poniżej znajduje się wykaz kontenerów, które będą dostarczone w ramach środowiska produkcyjnego, w wykazie ujęte zostały kontenery na potrzeby modułów które są objęte prawem opcji czyli ich wdrożenie uzależnione jest od decyzji zlecenia.

Tabela 12 Parametry kontenerów na środowisku produkcyjnym

Nazwa kontenera	vCPU	vRAM (GB)	HDD (GB)	Opis
React App Server	2	2,5	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
React App Server	2	2,5	50	Kontener odpowiedzialny za serwowanie statycznych danych aplikacji REACT
App admin	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu administracyjnego przez API
App e-learning	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu e-learning przez API. Moduł opcjonalny.
App webinary	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu webinary przez API. Moduł opcjonalny.
App konsorcjum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App konsorcjum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu konsorcjum przez API.
App repozytorium wiedzy	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
App repozytorium wiedzy	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu repozytorium wiedzy przez API.
Grafana	2	8	50	Kontener odpowiedzialny za obsługę monitorowania systemu we wszystkich aspektach.
App kontrole	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App kontrole	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu kontrole przez API.
App forum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.

App forum	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu forum przez API.
App wyszukiwarka orzeczeń KIO	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu wyszukiwarki orzeczeń KIO przez API.
App certyfikacja	2	2,5	50	Kontener odpowiedzialny za serwowanie danych do modułu certyfikacji przez API. Moduł opcjonalny.

5.4.5.5. INFRASTRUKTURA GLOBALNA (GLOBAL)

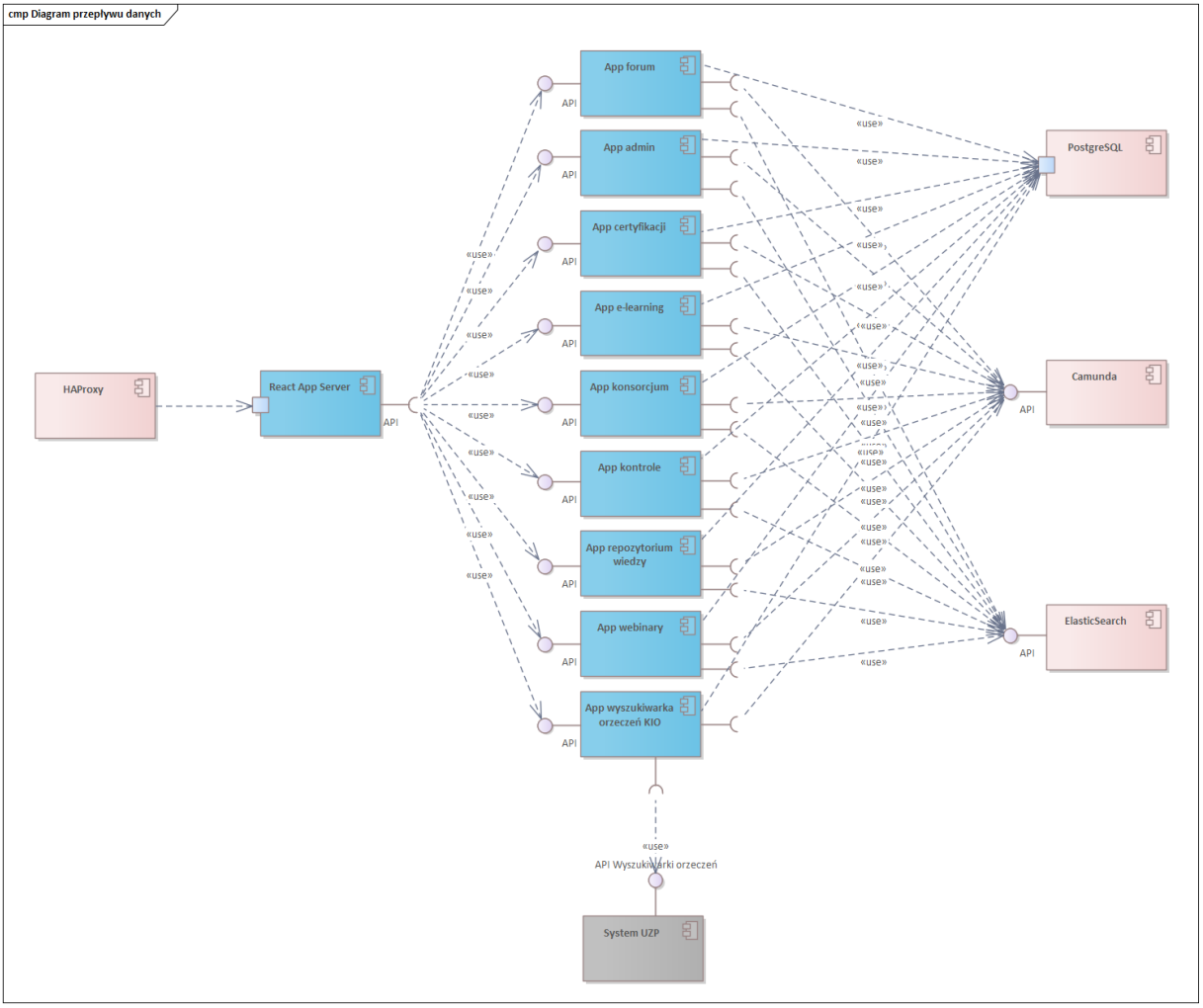
W ramach wszystkich środowisk wykorzystywane będą zasoby globalne opisane w tym rozdziale – są to serwery o zastosowaniu między środowiskowym. W skład tej grupy wchodzą wyłącznie serwery wirtualne z zainstalowanym oprogramowaniem dedykowanym. Wyszczególnić tu można 3 rodzaje serwerów – są to dwa serwery pocztowe, jeden serwer repozytorium oraz jeden serwer danych analitycznych. Przewidziane tu zostały dwa serwery pocztowe – jeden serwer produkcyjny, do którego podłączone zostanie tylko środowisko produkcyjne oraz jeden serwer testowy, który będzie obsługiwał wszystkie pozostałe środowiska. W przypadku serwera pocztowego testowego zastosowane zostaną reguły, dzięki którym poczta wychodząca będzie docierać tylko do wybranych grup odbiorców, ma to zabezpieczyć przed wysyłaniem poczty do zewnętrznych odbiorców, których adresy mailowe zostały użyte w celach testowych. Serwer repozytorium kodów i obrazów będą służyły do tworzenia pakietów instalacyjnych i obrazów za pośrednictwem procesów CI/CD. W ramach tego serwera skonfigurowane zostanie środowisko kompilacji kodów aby zminimalizować rozmiar środowiska – wyeliminować nadmiarowe maszyny wirtualne, które służyły by do kompilacji lub przygotowania kodów i obrazów. Ostatnią z maszyn wirtualnych wchodzących w skład tej grupy jest serwer danych analitycznych – będzie ona pełniła rolę bazy danych zorientowanych na czasie – wszystkie dane są zapisane w kontekście czasu a sama baza danych jest zoptymalizowana pod kątem obsługi danych szeregów czasowych. Dzięki takiej budowie bardzo wydajnie operuje ona na danych w kontekście czasu, charakter danych przechowywanych w takich bazach jest skoncentrowany na przechowywaniu danych a nie ich modyfikacji w związku z czym są one bardzo mocno nastawione na odczyt.

5.4.6. ARCHITEKTURA POŁĄCZEŃ SIECIOWYCH

System PI PZ będzie składał się z 5 środowisk specjalizowanych oraz części ogólnej wspólnej dla wszystkich środowisk. W zakresie środowisk wchodzących w skład systemu można wymienić:

- Środowisko deweloperskie (DEV)
- Środowisko integracyjne (INT)
- Środowisko testowe (TEST)
- Środowisko przedprodukcyjne (PRE-PROD)
- Środowisko produkcyjne (PROD)

Organizację sieciową oraz schemat połączenia każdego z wymienionych środowisk opisano w kolejnych rozdziałach.
Na poniższym diagramie przedstawiony jest przepływ danych w systemie PI PZ.



Rysunek 10 Przepływ danych

6. ZAŁĄCZNIKI

Załączniki mogą zostać udostępniony do wglądu w siedzibie Zamawiającego po uprzednim złożeniu oświadczenia o poufności.

Załącznik nr 1 - MRiT_Polityka Bezpieczeństwa Informacji.pdf

Załącznik nr 2 - MRiT_Polityka bezpieczeństwa teleinformatycznego i cyberbezpieczeństwa.pdf

Załącznik nr 3 - MRiT_Zasady bezpieczeństwa informacji.pdf

Załącznik nr 4 - MRiT_Zasady projektowania i wytwarzania bezpiecznych systemów i oprogramowania.pdf

Załącznik nr 5 - MRiT_Zasady zarzadzania danymi uwierzytelniajacymi.pdf

Załącznik nr 6 – MRiT_Koncepcja techniczna Platformy Internetowej Polityki Zakupowej Państwa.pdf