Zapytanie ofertowe
Opis Przedmiotu Zamówienia

„Przeprowadzenie niezależnych testów bezpieczeństwa: Infrastruktury Teleinformatycznej, Aplikacji Web oraz Aplikacji Mobilnej Zintegrowanego Systemu Zarządzania Gminą”

Spis treści:

1 Opis przedmiotu zamówienia

1.1 Podstawowe informacje – ogólny opis zamówienia

1. Nazwa zamówienia: *„Przeprowadzenie niezależnych testów bezpieczeństwa: Infrastruktury Teleinformatycznej, Aplikacji Web oraz Aplikacji Mobilnej Zintegrowanego Systemu Zarządzania Gminą”.*

2. Zamówienie jest częścią projektu pn. *„Rozwój elektronicznych usług publicznych w Gminie Września”* realizowanego przez Gminę Września w ramach Wielkopolskiego Regionalnego Programu Operacyjnego (WRPO) na lata 2014-2020: Oś Priorytetowa 2: „Społeczeństwo informacyjne” Działanie 2.1 „Rozwój elektronicznych usług publicznych”, Poddziałanie 2.1.1 „Rozwój elektronicznych usług publicznych”. Zamówienie stanowi wykonanie zadania projektowego: „*Zadanie 6. „Przeprowadzenie niezależnych testów bezpieczeństwa”.*

3. Zamawiającym jest Gmina Września. Zamówienie realizowane będzie w siedzibie Zamawiającego: Urząd Miasta i Gminy Września, ul. Ratuszowa 1, 62-300 Września.

4. Przedmiot zamówienia obejmuje przeprowadzenie *„niezależnych testów bezpieczeństwa - grey box”* dla wdrażanego u Zamawiającego *Zintegrowanego Systemu Zarządzania Gminą tj. Systemu RATUSZ* w zakresie:

   4.1. Infrastruktury Teleinformatycznej Zamawiającego tworzącej środowisko uruchomieniowe Systemu obejmującej oprogramowanie: systemowe, narzędziowe, bazodanowe, w tym infrastrukturę serwerową i sieciową;

   4.2. Aplikacji web: Platformy (portalu) e-Urząd;

   4.3. Aplikacji Mobilnej i dedykowanego dla tego oprogramowania środowiska hostującego, zewnętrznego wobec Infrastruktury Technicznej Zamawiającego, o której mowa w pkt. 4.1 (zakres testów bezpieczeństwa dla środowiska hostującego jest ograniczony wyłącznie do nieinwazyjnego badania podatności).

5. Niezależne testy bezpieczeństwa będą prowadzone na „żywym” organizmie działającego Systemu w terminach niezakłócających jego normalną pracę, przy jednoczesnym zapewnieniu bezpieczeństwa wszystkich danych oraz infrastruktury technicznej Systemu.

   5.1. W uzgodnionym zakresie Zamawiający oczekuje od Pentestera przeprowadzenia testów inwazyjnych, które powinny potwierdzić podatność Systemu na atak lub oczekiwaną jego odporność.

6. Celem testów jest wykazanie zdolności Systemu do zagwarantowania:

   6.1. podstawowych cech bezpieczeństwa systemu teleinformatycznego w zakresie:

      6.1.1. rozliczalności i niezaprzeczalności zdarzeń systemowych oraz działań użytkowników Systemu,

      6.1.2. integralność danych,

      6.1.3. dostępu do danych i funkcji Systemu wyłącznie dla uprawnionych do tego użytkowników.

   6.2. spełnienie wymagań w zakresie ochrony danych osobowych, które z punktu widzenia przedmiotu testów powinny być traktowane, jako „dane wrażliwe”.

7. Zadaniem Pentestera jest wykazanie możliwości wykonania skutecznego ataku i przełamania zastosowanych przez autorów Systemu mechanizmów bezpieczeństwa w obszarze udostępnionych funkcji

i przetwarzanych danych Systemu, w tym w zakresie wykorzystywanej przez System Infrastruktury Teleinformatycznej Zamawiającego. W tym celu Zamawiający dopuszcza również możliwość badania podatności Systemu poprzez wykonanie ataku inwazyjnego.

8. Do realizacji zamówienia Pentester powinien wykorzystać narzędzia automatyzujące czynności w zakresie: prowadzenia analiz, badania podatności, przeprowadzenia testów bezpieczeństwa, jakie są dostępne w formie skanerów podatności oraz narzędzi do przeprowadzenia testów bezpieczeństwa np. w dystrybucji systemu Kali Linux. Nie mniej jednak, poza powyższym Zamawiający oczekuje od Pentestera również przeprowadzenia czynności badania oraz testów prowadzonych „ręcznie", które zdecydowanie rozszerzają zakres przypadków testowych oraz ujmują szerszy zakres oceny podatności Systemu na obszar nieujawnionych błędów, w tym również błędów projektowo - logicznych.

9. Testy bezpieczeństwa muszą zostać przeprowadzone zgodnie z poniższym harmonogramem:

   9.1. Etap.1 – Przygotowanie organizacyjno – techniczne realizacji zamówienia – w terminie nie dłuższym niż 3 dni robocze do daty zawarcia umowy.

   9.2. Etap.2 - Przeprowadzenie oceny bezpieczeństwa Infrastruktury Teleinformatycznej Zamawiającego - infrastruktury stanowiącej środowisko uruchomieniowe dla Systemu RATUSZ.

   9.3. Etap.3 - Przeprowadzenie testów bezpieczeństwa Aplikacji Web oraz Aplikacji Mobilnej, w tym opracowanie raportu z testów wraz z prezentacją oraz omówieniem wyników testów i wydanych rekomendacji – w terminie zgodnie z Ofertą Pentestera w terminie do … dni roboczych od daty zawarcia umowy.

      9.3.1. Jeżeli wykonanie Etapu 3 wymaga oceny, badania podatności w zakresie, jakie Zamawiający przewidział w ramach czynności Etapu 2, to ten zakres działań Pentester powinien przewidzieć do wykonania tak, aby zapewnić realizację Etapu 3 zgodnie z zdeklarowanym przez siebie w Ofercie terminem na wykonanie całości przedmiotu zamówienia w, tym Etapu 3.

   9.4. Etap.4 - Przeprowadzenie retestów bezpieczeństwa – testów regresyjnych bezpieczeństwa Aplikacji Web oraz Aplikacji Mobilnej, w tym opracowanie raportu z retestów wraz z prezentacją oraz omówieniem wyników retestów i wydanych rekomendacji – w terminie zgodnie z Ofertą Pentestera w terminie do … dni roboczych od daty gotowości systemu do retestów po okresie 7 dni kalendarzowych, jakie na czynności korekty ustalono w zobowiązaniach dostawcy – producenta Systemu RATUSZ.

      9.4.1. Warunki związane z przystąpieniem Pentestera do retestów w okolicznościach wskazanych powyżej reguluje projekt umowy.

      9.4.2. Raport z retestów powinien obejmować końcowe wyniki prac wszystkich etapów, w tym z Etapu.2 obejmującego ocenę bezpieczeństwa Infrastruktury Teleinformatycznej Zamawiającego.

10. Działania w zakresie etapów: Etap.1, Etap.2 i Etap.3 Pentester powinien prowadzić równolegle w tym samym czasie – i w takim zakresie tak, aby zapewnić możliwość zaprezentowania (łącznego) raportu z testów bezpieczeństwa Etapu 2 w terminie określonym w Ofercie.

11. Celem zapewnienia sprawnej organizacji w zakresie prowadzenia testów bezpieczeństwa Pentester jest zobowiązany do koordynacji działań i uzgodnień w zakresie planowanych prac oraz w trakcie realizacji testów, dotyczy to w szczególności przygotowania, przeprowadzenia testów i związanych z tym uzgodnień technicznych oraz ustalenia terminów wykonania testów. Działania te Pentester powinien prowadzić z osobami wskazanymi przez Zamawiającego do bezpośredniej współpracy w realizacji zamówienia.

    11.1. Wszelkie ustalenia, wyjaśnienia, w tym dodatkowe pytania np. dot. infrastruktury teleinformatycznej poddawanej testom Systemu RATUSZ, jakie pojawią się w okresie realizacji zamówienia powinny być kierowane do Zamawiającego, przy czym dla usprawnienia realizacji zamówienia Zamawiający może

dopuścić bezpośrednią komunikację z Wykonawcą Systemu RATUSZ, w tym korespondencję elektroniczną, o ile w każdym przypadku zostanie powiadomiony o podjętych ustaleniach przez Pentestera i Wykonawcę.

12. Opis infrastruktury teleinformatycznej poddawanej testom „grey box" został zawarty w Załączniku nr 1 – „Opis Infrastruktury Teleinformatycznej poddawanej testom".

13. Warunki zdalnego dostępu do infrastruktury teleinformatycznej Zamawiającego oraz kwestie dot. udostępniania zasobów na potrzeby przeprowadzenia testów bezpieczeństwa z wewnątrz infrastruktury określa Załącznik nr 2 – „Warunki dostępu zdalnego do infrastruktury teleinformatycznej, w tym dostępne zasoby".

14. W realizacji zamówienia Pentester powinien uwzględnić poniższe uwarunkowania dotyczące sposobu wykonania:

    14.1. Zamawiający dopuszcza możliwość realizacji zamówienia przez Wykonawcę drogą elektroniczną w sposób zdalny w formie telekonferencji oraz poprzez zdalny dostęp do Infrastruktury Technicznej Zamawiającego, o ile zakres usług, co do ich rodzaju, będzie możliwy do wykonania w ten sposób oraz, o ile wcześniej zostanie to uzgodnione i zaakceptowane przez Zamawiającego.

        14.1.1. W tym celu dla realizacji części zadań związanych ze wykonaniem usługi w formie zdalnej Pentester zapewni dostępność dedykowanego rozwiązania do komunikacji na odległość. Koszt takiej usługi / oprogramowania jest w całości po stronie Pentestera.

        14.1.2. W przypadku dostępu zdalnego do Infrastruktury Technicznej Zamawiający zapewni Pentestera czasowy dostęp do licencji klienta oprogramowania VPN. Dostęp poprzez usługi VPN będzie zapewniony Pentestera wyłącznie w przypadku spełnienia określonych warunków organizacyjnych, jakie określa m.in. Załącznik nr 2 - „Warunki dostępu zdalnego do infrastruktury teleinformatycznej, w tym dostępne zasoby".

        14.1.3. W zakresie minimum Zamawiający oczekuje przynajmniej dwóch bezpośrednich spotkań z wykonawcą usługi, które miałby służyć budowaniu kompetencji po stronie Zamawiającego z zakresu zagadnień dot. testów bezpieczeństwa.

15. W wykonaniu zamówienia Pentester musi uwzględnić wszystkie wymagania i informacje, jakie zostały zawarte w niniejszej specyfikacji, w tym także wydawane na bieżąco zalecenia Zamawiającego stanowiące wyłącznie doprecyzowanie sposobu realizacji zamówienia i jego przedmiotu.

16. Pentester powinien zapewnić Zamawiającemu możliwość otrzymania informacji nt. stanu realizacji podczas spotkania projektowego, ale także zamówienia na jego wniosek Zamawiającego. Informację taką Pentester powinien przekazać w terminie nie później niż 2 dni roboczych od daty przedłożenia wniosku.

17. Zamawiający zaznacza, iż Pentester ponosi pełną odpowiedzialności za szkody, jakie mogą powstać wskutek:

    17.1. działania bez zgody i stosownych uzgodnień z Zamawiającym,

    17.2. błędów podczas przeprowadzonych testów, które doprowadziły do uszkodzenia infrastruktury technicznej, systemowej lub aplikacyjnej Zamawiającego, co nie stanowiło przedmiotu i celu prowadzonych testów,

    17.3. omyłkowych czynności Pentestera w obszarze infrastruktury technicznej nieprzewidzianym do przeprowadzenia testów (np. wykonanie testów inwazyjnych dla adresów IP spoza zakresu ustalonego przez Zamawiającego).

18. W przypadku, o którym mowa powyżej Pentester jest zobowiązany do usunięcia powstałej szkody siłami własnym lub zlecając niezbędne działania naprawcze na własny koszt odpowiednim podmiotom.

1.2 Wymagania prawne, normy techniczne, standardy i zalecenia

1. W realizacji zamówienie Pentester powinien uwzględnić obowiązujące Zamawiającego przepisy prawa. Odnosi się to do wymagań, jakie powinien spełniać dostarczany przez Wykonawcę System RATUSZ. W przypadku zobowiązań Pentestera odnosi się to do kwestii wydania rekomendacji w raporcie z testów, który powinien uwzględniać nie tylko „czysty" aspekt techniczny wydawanych zaleceń, ale także powinien uwzględniać w tym zakresie (o ile jest niezbędne) obowiązujące Zamawiającego przepisy prawa, o ile odnoszą się one do implementacji określonego rozwiązania lub użycia wskazanych przez te przepisy metod lub technik. Chodzi o to, aby rekomendacje, były zgodne, lub, co najmniej niesprzeczne z obowiązującymi przepisami prawa, m. in. takimi jak:

    1.1. Przepisy krajowe:

        1.1.1. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. 2021 r., poz. 1797);

        1.1.2. Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344) wraz z aktami wykonawczymi, w tym:

            1.1.2.1. Rozporządzenie Ministra Cyfryzacji z dnia 10 marca 2020 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do uwierzytelniania użytkowników (Dz.U. z 2020 r., poz. 399);

        1.1.3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070 ze zm.) wraz z aktami wykonawczymi, w tym:

            1.1.3.1. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t. j. Dz.U. z 2017 r. poz. 2247);

            1.1.3.2. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t. j. Dz. U. z 2018 r. poz. 180);

            1.1.3.3. Rozporządzenie Rady Ministrów z dnia 27 września 2005 r. w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (t. j. Dz. U. z 2018 r. poz. 29);

            1.1.3.4. Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2018 r. poz. 1750);

        1.1.4. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. z 2019 r. poz. 848 ze zm.);

        1.1.5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz.U.2020 1369 ze zm.);

        1.1.6. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781);

            1.1.6.1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) (Dz.U. 2016r. L 119/1);

2. Rozporządzenia Parlamentu Europejskiego:

   2.1.1. Rozporządzenie Parlamentu Europejskiego Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwanego dalej „RODO" (Dz. UE. L. 2016. 119. 1 z dnia 2016.05.04);

   2.1.2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, s. 73).

3. Ponadto, w realizacji zamówienia Pentester powinien uwzględnić zalecenia dot. stosowania norm oraz standardów technicznych w zakresie, jaki wynika z potrzeb prawidłowego wykonania zamówienia, co w szczególności może odnosić się do takich unormowań, jak: Polskie Normy (PN) wprowadzające z Sektora Technika informatyczna – Technika bezpieczeństwa lub norm równoważnych, jak:

   3.1.1. PN-EN ISO/IEC 27000: 2017-06 Systemy zarządzania bezpieczeństwem informacji -- Przegląd i terminologia,

   3.1.2. PN-EN ISO/IEC 27001: 2017-06 Systemy zarządzania bezpieczeństwem informacji – Wymagania,

   3.1.3. PN-ISO/IEC 27005: 2010 Zarządzanie ryzykiem w bezpieczeństwie informacji,

   3.1.4. PN-ISO/IEC 29151: 2019-01 Praktyczne zasady ochrony informacji o identyfikowalnych osobach,

   3.1.5. PN-ISO/IEC 29134: 2018-11 Wytyczne dotyczące oceny skutków dla prywatności.

4. Z punktu widzenia planowanych do przeprowadzenia niezależnych testów bezpieczeństwa, Pentester powinien uwzględnić wytyczne dot. sposobu przeprowadzenia testów bezpieczeństwa dla aplikacji WWW oraz Aplikacji Mobilnej, jakie są wydawane przez:

   4.1. Fundację non-profit OWASP (ang. Open Web Application Security Project) https://owasp.org/), co w szczególności dotyczy tzw. listy OWASP – Top Ten oraz Standardu Weryfikacji Bezpieczeństwa Aplikacji (ang. ASVS - Application Security Verification Standard), który określa grupy wymagań, wg których należy dokonać oceny podatności celem określanie rzeczywistego poziomu bezpieczeństwa danego rozwiązania.

      4.1.1. Zamawiający dla testów środowisk aplikacyjnych rekomenduje do testów poziom „2" ASVS, dla którego należy założyć, iż:

         4.1.1.1. występuje zgodność implementacji z architekturą, jaką wskazano w opisie specyfikacji,

         4.1.1.2. wdrożone przez producenta mechanizmy bezpieczeństwa powinny funkcjonować w sposób prawidłowy i zostały zaimplementowane odpowiednio do ich przeznaczenia, aby zagwarantować ustalony poziom bezpieczeństwa aplikacji, przyjmując, przy tym, iż przetwarzane dane obejmują i / lub mogą obejmować „dane wrażliwe";

         4.1.1.3. z oceny bezpieczeństwa – zgodnie z założeniami niniejszej specyfikacji, w tym sposobu przeprowadzenia testów „gray box" - na poziomie „2" wyłącza się ocenę kodu źródłowego aplikacji.

   4.2. SANS Technology Institute https://www.sans.org/emea/ (wymaganie opcjonalne).

1.3 Kluczowy z punktu widzenia celu obszar bezpieczeństwa – ochrona danych osobowych

1. Jednym z zasadniczych celów prowadzenia niezależnych testów bezpieczeństwa jest ocena bezpieczeństwa danych osobowych, jakie będą gromadzone i przetwarzane w Systemie.

2. Zamawiający oczekuje od wykonawcy testów szczególnej uwagi na zagadnienia ochrony – bezpieczeństwa danych osobowych, w których to kluczową rolę ogrywają "Wytyczne 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25" - opracowanie przez Europejską Radę Ochrony Danych (EROD) https://uodo.gov.pl/pl/414/1331.

3. W wydanych w raportach rekomendacjach Zamawiający wymaga, aby Pentester:

   3.1. wydał ocenę poziomu zidentyfikowanych zabezpieczeń w zakresie ochrony danych z punktu widzenia „obowiązku ochrony danych w fazie projektowania oraz domyślnej ochrony danych”, co zgodnie z wytycznymi 4/2019 obejmuje nie tylko nowe, projektowane systemy teleinformatyczne, ale także już opracowane i działające (ww. wytyczne pkt. 96 triet 10).

   3.2. wydał ewentualne rekomendacje dot. metod i technik zabezpieczenia danych osobowych do Polityki Ochrony Danych Osobowych, jaką prowadzi Zamawiający oraz będących w przygotowaniu założeń do Systemu Zarzadzania Bezpieczeństwem Informacji (SZBI).

4. Prowadzone testy inwazyjne przez Pentestera powinny być ukierunkowane na kontrolowany dostęp do danych osobowych lub ich modyfikację (dotyczy to w szczególności danych osobowych oraz powiązanych z nimi danych, jakie mogą być dostępne w portalu e-urząd, jak zobowiązania finansowe, płatności, korespondencja).

2 Realizacja zamówienia – etapy i oczekiwane rezultaty

2.1 Etap.1 Przygotowane organizacyjno – techniczne realizacji zamówienia

1. W ramach czynności tego etapu Pentester powinien uzgodnić z Zamawiającym optymalny z punktu widzenia celu przedmiotu zamówienia – sposób realizacji zamówienia, co odnosi się do kwestii:

   1.1. Zdefiniowania harmonogramu realizacji zamówienia tj. terminów poszczególnych testów bezpieczeństwa oraz oceny podatności w sposób „nieinwazyjny", niezakłócający pracy użytkowanych systemów aplikacyjnych Zamawiającego tj. Systemu RATUSZ.

      1.1.1. Zamawiający dopuszcza możliwość przeprowadzenia testów penetracyjnych w formie rzeczywistej symulacji ataku hakera, w ramach, którego może dojść do utraty cech integralności danych, niezaprzeczalności zdarzeń systemowych w szczególności w obszarze przetwarzania danych osobowych. Przeprowadzenie tego rodzaju testów musi być każdorazowo uzgodnione z Zamawiającym tak, aby służby informatyczne Zamawiający były przygotowane na takie zdarzenie.

   1.2. Określenia zasad organizacyjno – technicznych dot. obustronnej komunikacji oraz dostępu do Infrastruktury Teleinformatycznej Zamawiającego, o ile ustalenia zawarte w niniejszej specyfikacji i w umowie są niewystarczające i wymagają dodatkowego doprecyzowania, jak chociażby w kwestii dot. bezpośredniej komunikacji i podania danych kontaktowych osób odpowiedzialnych za techniczną realizację zamówienia po stronie Pentestera oraz odpowiednie współdziałanie po stronie Zamawiającego.

   1.3. Uzgodnienia i zamodelowania potencjalnych innych zagrożeń / podatności, jakie nie zostały w sposób jawny wskazane przez Zamawiającego w niniejszej specyfikacji, a mogą ujawnić się w infrastrukturze aplikacyjnej i systemowej Systemu RATUSZ. Dotyczy to przypadków, których Zamawiający nie mógłby określić lub wskazać bez czynnego udział, konsultacji i sugestii doświadczonego Pentestera w procesie przygotowania organizacyjno – technicznego testów.

2. Uzgodnienia dot. sposobu realizacji zamówienia powinny być zawarte w formie „Notatki" obustronnie podpisanej przez Przedstawicieli Stron umocowanych w Umowie.

3. Wybór kolejności poszczególnych działań z punktu widzenia celu zamówienia leży w decyzji wykonawcy testów, który jako profesjonalny podmiot realizujący tego rodzaju usługi, posiadający doświadczenie w wykonywaniu takich zamówień jest w stanie dokonać właściwego, optymalnego podziału i kolejności zadań, podzadań tak, aby optymalnie zrealizować zamówienie i zapewnić oczekiwane przez Zamawiającego rezultaty przypisane do wyróżnionych logicznych etapów realizacji zamówienia.

   3.1. Powyższe dotyczy m. in. realizacji etapów: Etap.2 i Etap.3, które mogą być w opinii Zamawiającego równocześnie.

      3.1.1. Uwaga ta nie dotyczy testów bezpieczeństwa dla Aplikacji Mobilnej, dla której to środowisko hostujące jest poza Infrastrukturą Techniczną Zamawiającego.

   3.2. Wszystkie wyniki przeprowadzonych badań podatności oraz testów bezpieczeństwa muszą zostać zawarte w „Raporcie z badania, oceny podatności oraz wyników testów bezpieczeństwa" o ustalonej strukturze, jaką określono w Rozdziale 2.5.

4. Testy bezpieczeństwa powinny być prowadzone:

4.1. w środowisku produkcyjnym Systemu, jakie zostało udostępnione przez Zamawiającego.

4.2. po godzinach pracy urzędu oraz, o ile będzie to możliwe, za zgodą Zamawiającego również w okresie dni wolnych od pracy, w szczególności dotyczy to przeprowadzenia testów inwazyjnych.

5. Testy nieinwazyjne oraz badanie podatności, w tym ocena konfiguracji Infrastruktury Teleinformatycznej Zamawiającego mogą być prowadzone za zgodą Zamawiającego w dni robocze i w czasie pracy urzędu (7.00-15.00).

6. Każdorazowo przed przystąpieniem do testów inwazyjnych lub działań mogących skutkować utratą stabilności Systemu, czy też integracji danych, Zamawiający zgodnie z ustaleniami z Pentesterem zapewni utworzenie kopii baz danych oraz środowiska produkcyjnego dla wszystkich uruchomionych maszyn wirtualnych stanowiących Infrastrukturę Teleinformatyczną Systemu. Po przeprowadzeniu testów – wg podjętych ustaleń z Pentesterem, Zamawiający dokona pełnego odtworzenia środowiska produkcyjnego.

2.2 Etap.2 Przeprowadzenie oceny bezpieczeństwa Infrastruktury Teleinformatycznej Zamawiającego

1. Badanie bezpieczeństwa Infrastruktury Teleinformatycznej Zamawiającego stanowiącej środowisko uruchomieniowe dla Systemu RATUSZ może zostać przeprowadzone odrębnie lub, jako działanie połączone z testami bezpieczeństwa dla Aplikacji Web Systemu RATUSZ, co może być zgodne z metodykami prowadzenia testów bezpieczeństwa, w których to wyodrębnia się tzw. fazę rozpoznania. Zakres niezbędnych działań i oceny podatności związany z realizacją Etapu 3 leży w gestii wyboru i decyzji Pentestera.

2. Przedmiot badania i oceny w zakresie bezpieczeństwa Infrastruktury Teleinformatycznej Zamawiającego stanowiącej środowisko uruchomieniowe dla Systemu RATUSZ, obejmuje, co najmniej:

2.1. Analizę topologii sieci komputerowej:

2.1.1. Celem tego zadania jest analiza logicznej i fizycznej topologii sieci oraz reguł kierowania ruchem sieciowym. Do analizy należy brać pod uwagę urządzenia aktywne i ich zadania w zakresie kierowania i obsługi ruchu sieciowego, a także wszystkie urządzenia budujące topologię sieci: routery, systemy firewall, przełączniki sieciowe, elementy systemu IDS.

2.1.2. W wyniku badania należy dokonać oceny:

2.1.2.1. konstrukcji topologii sieci pod kątem ogólnych zasad budowy tego typu rozwiązania,

2.1.2.2. topologii pod kątem zasięgu ruchu sieciowego w poszczególnych segmentach sieci,

2.1.2.3. topologii sieci pod kątem niezawodności i redundancji poszczególnych jej elementów,

2.1.2.4. topologii pod kątem możliwości przeprowadzenia ataku zdalnego,

2.1.2.5. potencjalnych celów ataku i źródeł ataków,

2.1.2.6. możliwości zwiększenia poziomu bezpieczeństwa sieci poprzez zmiany konfiguracji i / lub topologii sieci.

2.2. Analizę usług systemowych:

2.2.1. Celem tego zadania jest analiza usług systemowych udostępnianych w obszarze poddanym badaniu, co obejmuje:

2.2.1.1. usługi uruchomione na potrzeby Systemu,

2.2.1.2. usługi wymagane dla zapewnienia identyfikowanej funkcjonalności,

2.2.1.3. analizę ruchu sieciowego przepływającego pomiędzy segmentami sieci, jaki jest generowany w wyniku działania usług systemowych,

2.2.1.4. identyfikację usług systemowych uruchomionych nadmiarowo i / lub stwarzających realne niebezpieczeństwo ataku.

2.3. Analizę konfiguracji urządzeń aktywnych:

2.3.1. Celem tego zadania jest przeprowadzenie przeglądu konfiguracji sprzętowej i programowej wszystkich urządzeń aktywnych wchodzących w skład Infrastruktury Teleinformatycznej obsługującej ruch sieciowy badanego Systemu, co obejmuje:

2.3.1.1. identyfikację komponentów wymagających uaktualnienia oraz instalacji poprawek systemowych, co odnosi się do podatności oprogramowania wewnętrznego urządzeń (tzw. systemów operacyjnych urządzeń aktywnych) oraz powiązanego z tym oprogramowania systemów operacyjnych hostów,

2.3.1.2. ocenę poprawności konfiguracji: routerów i serwerów dostępowych, przepływów dla systemów firewall, elementów systemu IDS, przełączników sieciowych,

2.3.1.3. ocenę konsoli zarządzających z puntu widzenia zakresu możliwości konfiguracji urządzeń,

2.3.1.4. ocenę systemów operacyjnych poszczególnych urządzeń aktywnych systemu.

2.4. Analizę konfiguracji hostów (serwerów fizycznych) oraz maszyn wirtualnych:

2.4.1. Celem zadania jest badanie i ocena bezpieczeństwa serwerów oraz maszyn wirtualnych, co obejmuje:

2.4.1.1. badanie poprawności konfiguracji systemów operacyjnych oraz ich administracji pod względem bezpieczeństwa;

2.4.1.2. identyfikację podatności, czyli luk bezpieczeństwa przy wykorzystaniu narzędzi do badania podatności (ang. vulnerability scanner).

2.5. Analizę zastosowanych rozwiązań w zakresie komunikacji wewnętrznej i zewnętrznej w zakresie zapewnienia poufności danych:

2.5.1. Celem zadania jest ocena zastosowanych rozwiązań zapewaniających minimalny poziom poufności przesyłanych i gromadzonych danych. Analizie podlegać będą rozwiązania zaimplementowane w Systemie takie, jak: wykorzystanie protokołu szyfrującego SSL, TLS (szyfrowanie asymetryczne, certyfikaty X.509) lub połączenia VPN. Poza tym ocenie podlegać będzie też zakres zastosowania np. do uwierzytelnienie serwera, a niekiedy również klienta usługi.

2.6. Analizę przepływności sieci:

2.6.1. Celem zadania jest ocena przepływności ruchu pomiędzy strefami bezpieczeństwa z uwzględnieniem podziału na wydzielone strefy serwerów bazy danych, serwerów aplikacji DMZ (i inne) z uwzględnieniem wyników weryfikacji poziomu logowania na urządzeniach brzegowych (firewall) dla sesji nawiązywanych pomiędzy krytycznymi strefami bezpieczeństwa.

2.7. Analizę systemu monitorowania ruchu:

2.7.1. Celem zadania jest ocena dostępnych, zaimplementowanych rozwiązań w zakresie systemu monitorowania ruchu dla segmentów sieci wystawionych na ataki z zewnątrz. Testy powinny być przeprowadzone w obszarach krytycznych na styku połączeń: sieć Internet – strefa DMZ, strefa DMZ - serwery aplikacyjne, serwery aplikacyjne – serwery baz danych.

2.8. Przeprowadzenie testów bezpieczeństwa z obszaru infrastruktury:

2.8.1. Celem tego zadania jest ocena odporności Infrastruktury Teleinformatycznej Systemu na wystąpienie określonych zdarzeń spowodowanych m.in. przez symulowane ataki. Zakres tego zadania obejmuje:

2.8.1.1. Przeprowadzenie analizy penetracyjnej przez badanie konfiguracji infrastruktury „z zewnątrz" i ocenę podatności na próby penetracji dostępnych usług, przy czym działania te powinny być przeprowadzone z wykorzystaniem dedykowanych do tego celu skanerów sieciowych.

2.8.1.2. Wykonanie kontrolowanego włamania (ataku) przez przeprowadzenie włamania przy użyciu metod nieinwazyjnych oraz metod inwazyjnych w uzgodnieniu z Zamawiającym, co powinno pozwolić wykryć potencjalne luki w zabezpieczeniach Infrastruktury Teleinformatycznej Systemu.

3. Działania Pentestera na tym etapie muszą być udokumentowane w zakresie, jaki określone zostały przez potrzeby informacyjne raportu z testów Rozdział 2.5.

4. Zakres działań Pentestera w obszarze dot. Infrastruktury Teleinformatycznej Zamawiającego w ramach niniejszego etapu, a także testów w zakresie Etap.3 może zostać rozszerzony o zagadnienia, jakie Pentester wskaże, jako kluczowe do oceny stanu Infrastruktury Teleinformatycznej oraz aplikacyjnej Systemu RATUSZ podczas prac przygotowawczych w zakresie tzw. modelowania testów, o czym mowa w Rozdz. 2.1 pkt. 1.3, Rozdz. 2.3.1 pkt. 3.

2.3 Etap.3 Przeprowadzenie testów bezpieczeństwa Aplikacji Web oraz Aplikacji Mobilnej

1. Przedmiotem badania oraz oceny podatności będą Aplikacja Web oraz Aplikacja Mobilna Systemu RATUSZ oraz w ograniczonym zakresie środowisko uruchomieniowe – hostujące Aplikacji Mobilnej.

2. Opis działania Aplikacji Web, Aplikacji Mobilnej zawiera zewnętrzny do niniejszej specyfikacji:

2.1. Załącznik nr 4 - Aplikacja Web – Platforma (portal) e-Urząd;

2.2. Załącznik nr 5 – Aplikacja Mobilna.

3. Testy bezpieczeństwa dla ww. aplikacji powinny obejmować m.in:

3.1.1. badanie luk oprogramowania w szczególności w zakresie:

3.1.1.1. możliwości podniesienia poziomu uprawnień uwierzytelnionego lub anonimowego użytkownika,

3.1.1.2. przejęcie danych uwierzytelniania lub sesji kont innych użytkowników,

3.1.1.3. uzyskania nieautoryzowanego dostępu do danych lub nieuprawnionej zmiany danych,

3.1.1.4. przejęcia kontroli działania usług;

3.1.1.5. zablokowania działania usług,

3.1.1.6. uruchomienia innych usług nieujętych w specyfikacji / konfiguracji Systemu,

3.1.2. wykrycia wszelkich podatności mających wpływ na dostępność, poufność oraz integralność danych.

2.3.1 Testy Aplikacji Web

1. Zakres testów bezpieczeństwa (testów penetracyjnych) dla Aplikacji Web obejmie, co najmniej 20 testów bezpieczeństwa, w tym 10 testów z aktualnej listy dziesięciu najpopularniejszych ataków sieciowych tzw. OWASP TOP 10 https://owasp.org/www-project-top-ten/ oraz 10 niepokrywających się testów z „top ten" z poniższej listy:
    1.1. Test penetracyjny styku z Internetem (przy konfiguracji produkcyjnej) – w tym skuteczności urządzeń IDS/IPS.
    1.2. Manipulacje parametrami.
    1.3. Techniki podsłuchu i manipulowania transmisją (w tym Man in The Middle).
    1.4. Wywołanie strony serwisu spoza ścieżki przewidzianej przez projektantów aplikacji (Forcefull browsing).
    1.5. Atak Path Traversal.
    1.6. Technika Google Hacking (dotyczy aplikacji opublikowanych w sieci Internet).
    1.7. Filtrowanie danych wejściowych.
    1.8. Omijanie filtrowania danych wejściowych i wyjściowych.
    1.9. Ataki na sesję aplikacji webowej (session fixation i session adoption).
    1.10. Ataki typu Injection (np. SQL/XML/XPath/HTML/LDAP oraz innych zgodnie z technologią aplikacji) i Blind SQL Injection.
    1.11. Ataki XSS - Cross Site Scripting (persistent, reflected, itp.), czyli osadzenie obcego skryptu.
    1.12. Niepoprawna obsługa uwierzytelniania i sesji.
    1.13. Niezabezpieczone bezpośrednie odwołanie do obiektu (Insecure Direct Object References).
    1.14. Fałszowanie żądań (CSRF - Cross Site Request Forgery).
    1.15. Niepoprawne ustawienia (Security Misconfiguration).
    1.16. Brak zabezpieczeń dostępu przez URL (Failure to Restrict URL Access).
    1.17. Brak walidacji przekierowań (Unvalidated Redirects and Forwards).
    1.18. Błędy szyfrowania danych (Insecure Crytptographic Storage).
    1.19. Niedostateczne zabezpieczenia wymiany danych (Insufficent Transport Layer Protection).
    1.20. Atak typu brute force (sprawdzenie czy konto lub adres IP zostanie zablokowane).
    1.21. Testy dotyczące ujawniania informacji o środowisku hostującym.
    1.22. Testy typu DoS (np. flooding).
    1.23. Ataki typu spoofing.
    1.24. Ocena kompletności zbieranych informacji w logach.
    1.25. Ataki w celu rozpoznania aplikacji i platformy.
    1.26. Próba podniesienia uprawnień.

1.27. Przekazanie wrażliwych danych w adresie URL lub podmiana wartości parametrów UR.

1.28. Modyfikacje treści strony w aplikacji internetowej.

1.29. Wymuszenie kodów błędów HTTP500, czy też HTTP400, HTPP300, aby uzyskać informacje o strukturze katalogów serwera WWW.

1.30. Zdradzenie nadmiarowych danych np. nazwy i wersji serwera aplikacji.

1.31. Nawiązywanie równoległych połączeń przy tych samych danych użytkownika (login / hasło), czy też dopuszczenie do próby obejścia zastosowanych zabezpieczeń np. blokada konta po nieudanych próbach logowania itp.

2. Test bezpieczeństwa z listy OWASP TOP 10 powinny być przeprowadzone w oparciu o wszystkie scenariusze testowe, jakie zostały opisane w przedmiotowych wytycznych.

3. Poza powyższym na podstawie wytycznych OWASP Testing Guide Pentester zaproponuje oraz uzgodni z Zamawiającym i przeprowadzi jeszcze min. pięć (5) testów odpowiednio dobranych do specyfiki Aplikacji Web dokonując wyboru testów i oceny podatności np. o których mowa w publicznie dostępnych bazach takich, jak: www.exploit-db.com, www.rapid7.com, www.wuldb.com. Działania te wchodzą w zakres zamodelowania potencjalnych innych zagrożeń / podatności, jakie nie zostały w sposób jawny wskazane przez Zamawiającego w niniejszej specyfikacji.

2.3.2 Testy Aplikacji Mobilnej

1. Zakres testów bezpieczeństwa (testów penetracyjnych) dla Aplikacji Mobilnej obejmie identyfikację podatności z aktualnej listy podatności OWASP TOP 10 dla aplikacji mobilnych https://owasp.org/www-project-mobile-top-10/, co na dzień opracowania niniejszej specyfikacji obejmowało następujące podatności:

   1.1. M1: Niewłaściwe użycie platformy

   1.2. M2: Niebezpieczne przechowywanie danych

   1.3. M3: Niepoprawna komunikacja

   1.4. M4: Niepoprawne uwierzytelnianie

   1.5. M5: Niewystarczająca kryptografia

   1.6. M6: Niepewna autoryzacja

   1.7. M7: Jakość kodu klienta (podatność wyłączona z zakresu testów)

   1.8. M8: Manipulowanie kodem

   1.9. M9: Inżynieria wsteczna

   1.10. M10: Zewnętrzna funkcjonalność

2. Testy Aplikacji Mobilnej powinny być prowadzona na podstawie wytycznych zawartych w publikacji OWASP: MASTG (ang. Mobile Application Security Testing Guide) i MASVS (ang. Mobile Application Security Verification Standard).

2.4 Etap.4 - Przeprowadzeniem retestów bezpieczeństwa, wnioski końcowe

1. Retesty powinny być przeprowadzone w pełnym zakresie wymagań, jaki określa Etap.2.
2. Retesty nie mogą dotyczyć wyłącznie testów regresywnych dla przypadków testowych, w których zidentyfikowano podatności wskazane do korekty / naprawy.
3. Retesty kończy opracowanie raportu.

2.5 Zakres informacyjny raportów, udokumentowanie wyników

1. Zamawiający oczekuję opracowania dwóch raportów z przeprowadzonych analiz, badań podatności oraz testów bezpieczeństwa, przy czym dopuszcza się opracowanie raportu z retestów w formie aktualizacji pierwszego raportu z testów. W takim przypadku opisy dot. przypadków testowych dla zidentyfikowanych podatności muszą czytelnie wyróżniać uzyskane wyniki w fazie testów oraz retestów.
2. Każdy z raportów powinien obejmować następujące treści:
   - 2.1. Metryka dokumentu
   - 2.2. Opis skrócony dla Kierownictwa
   - 2.3. Opis zastosowanych metod i technik w zakresie analizy, badania podatności i testów (wskazane odwołanie do dokumentów źródłowych)
   - 2.4. Opis skrócony przeprowadzonych analiz, badań podatności, testów bezpieczeństwa odpowiednio do zakresu przedmiotowego niniejszej specyfikacji.
   - 2.5. Opis badań Infrastruktury Teleinformatycznej oraz uzyskanych wyników i powiązanych z tym rekomendacji w zakresie, w jakim wskazane to zostało w Rozdziale 2.2, w układzie odpowiednio do poszczególnych obszarów badania (Rozdz. 2.2 podpunkty od 2.1 do 2.8)
   - 2.6. Opis przypadków testowych testów bezpieczeństwa zawierający:
     - 2.6.1. rozdział / numer wymagania niniejszej specyfikacji,
     - 2.6.2. umiejscowienie podatności (Infrastruktura Teleinformatyczna, Aplikacja Web / Aplikacja Mobilna: komponent, funkcja / operacja),
     - 2.6.3. warunki brzegowe,
     - 2.6.4. opis podatności,
     - 2.6.5. dowody (zrzut ekranu, załącznik do raportu w formie wydruku, link URL, inne),
     - 2.6.6. poziom zagrożeń – ocena poziomu krytyczności podatności wg. wybranego przez wykonawcę testów systemu klasyfikacji podatności na zagrożenia, przy czym rekomendowany przez Zamawiającego do zastosowania system oceny istotności zagrożeń to CVSS (ang. Common Vulnerability Scoring System) w wersji 3.1 (lub 4.0) włącznie z użyciem kalkulatora online https://www.first.org/cvss/calculator/3.1
     - 2.6.7. szczegółowe rekomendacje dot. sposobu usunięcia / naprawy podatności.
   - 2.7. Opcjonalnie – opis rozbieżności pomiędzy specyfikacją infrastruktury teleinformatycznej wskazaną w niniejszym opisie przedmiotu zamówienia w zakresie obszarów poddanych testom, a zidentyfikowaną podczas badania podatności
   - 2.8. Podsumowanie ilościowe i jakościowe wyników z testów

2.9. Wnioski końcowe uwagi i rekomendacje.

3. Zamawiający dopuszcza uzgodnienie z wykonawcą testów innej struktury raportu, w tym w szczególności innego sposobu opisu przypadków testowych / podatności, który zapewnieni jemu oczekiwany z punktu widzenia celu określony, wymagany zakres rzeczowy informacji.

4. Raport końcowy po retestach musi zawierać dodatkowo oświadczenia:

   4.1. Oświadczenie imienne każdego z członków zespołu o zachowaniu poufności zrealizowanego zamówienia, w tym wszelkich udostępnionych przez Zamawiającego informacji i materiałów.

   4.2. Oświadczenie Pentestera o zachowaniu poufności oraz o usunięciu wszystkich kopii danych, dokumentów oraz wszelkich materiałów, które znalazły się w jego władaniu w okresie realizacji zamówienia. Do oświadczenie należy dołączyć protokół zniszczenia kopii materiałów i dokumentów.

5. Każdy z opracowanych przez Pentestera raportów, jako dokumentacja z realizacji zamówienia - posiada status informacji poufnej.

6. Zamawiający wymaga, aby wszystkie opracowane dokumenty (raporty) charakteryzowały się wysoką jakością, na którą będą miały wpływ takie czynniki jak:

   6.1. Struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób,

   6.2. Zachowanie standardów w zakresie sposobu pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu,

   6.3. Kompletność dokumentu, rozumiana, jako pełne, bez wyraźnych braków, przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia,

   6.4. Spójność i niesprzeczność dokumentu, rozumianych, jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.

7. Ww. kryteria jakościowe Zamawiający będzie brał pod uwagę podczas procedury odbioru wyników testów w zakresie dot. oceny przedmiotu opracowania raportu.

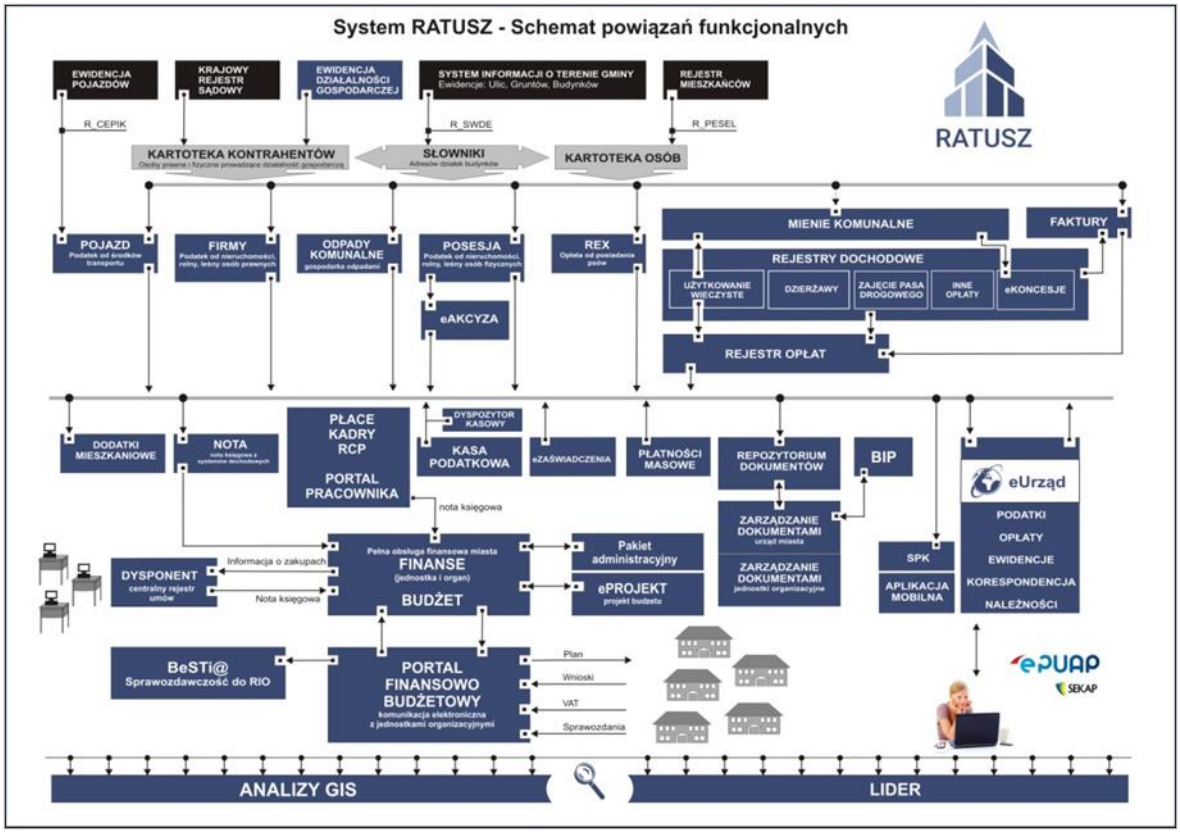
3 Załącznik nr 1 – Opis Infrastruktury Teleinformatycznej poddawanej testom

Informacje nt. adresacji IP obszarów poddawanych testom Zamawiający, a także instrukcję użytkownika Aplikacji Mobilnej Zamawiający - udostępni wykonawcy testów po zawarciu umowy.

3.1 System RATUSZ – Platforma (portal) e-Urzad

System RATUSZ to dedykowany dla Jednostek Administracji Samorządowej (JST) zintegrowany system informatyczny do zarządzania, inaczej Zintegrowany System Zarządzania Gminą (ZSZG). W skrócie w odniesieniu do całościowej infrastruktury aplikacyjnej i systemowej w niniejszym opracowaniu (ZSZG) będzie przywoływany, jako - System.

System RATUSZ wdrażany w Urzędzie Miasta i Gminy Września System RATUSZ obejmuje wiele rozwiązań aplikacyjnych, które cechuje różnorodność technologiczna. Architekturę logiczną Systemu przedstawia poniższy ideogram.



Infrastrukturę techniczną Systemu RATUSZ, opartą o udostępnione przez Zamawiającego te same, co do rodzaju zasoby techniczne, jakie wskazano do dyspozycji Pentestera - stanowi: siedem (7) maszyn wirtualnych VM, których częściową specyfikację zawiera poniższa tabela.

	Bazodanowy FIREBIRD	Bazodanowy PostgreSQL	Serwer aplikacji wewnętrzny 2W/3W	Serwer aplikacji wewnętrznych udostępnianych na zewnątrz bez VPN	PORTAL Finansowo budżet.	Serwer EURZĄD warstwa pośrednia	Serwer EURZAD warstwa prezentacji
System operacyjny	Redhat 7/8 / CentOS 7/8	Redhat 7/8 / CentOS 7/8	Windows Server 2021	Windows Server 2021	Windows Server 2021	Windows Server 2021	Windows Server 2021
Serwer bazodanowy	Firebird	Postgresql oraz PostGIS 3	-	-	-	Firebird	-
pozostałe komponenty – oprogramowanie narzędziowe			- Serwer IIS 8.5 lub nowszy - .NET Framework 4.7.1 lub nowszy - NET Core 2.x IIS - Certyfikat SSL/HTTPS	- Serwer IIS 8.5 lub nowszy - .NET Framework 4.7.1 lub nowszy - NET Core 2.x IIS - Certyfikat SSL/HTTPS	- Serwer IIS 8.5 lub nowszy - .NET Framework 4.7.1 lub nowszy	- Serwer IIS 8.5 lub nowszy - .NET Framework 4.7.1 lub nowszy	- Serwer IIS 8.5 lub nowszy - .NET Framework 4.7.1 lub nowszy

Opis funkcjonalny Platformy (portalu) eUrzad poddawanej testom bezpieczeństwa zawiera zewnętrzny – Załącznik nr 4 do OPZ – opisujący funkcje platformy front-office.

3.2 Aplikacja Mobilna

Aplikacja Mobilna ma strukturę modułową i obejmuje dwa moduły (łącznie kilkanaście podstron):

- „Kiedy odpady", gdzie publikowany jest harmonogram odpadów;
- „Konsultacje – w kontakcie JST" gdzie zapewniony jest dostęp do publikowanych ogłoszeń.

Komunikacja pomiędzy modułami odbywa się poprzez osobne usługi API z wykorzystaniem proxy Cloudflare. Wszystkie usługi API są hostowane są na klastrze, jako usługi Kubernetes service (składającym się z 3 maszyn wirtualnych). Komunikacja między API a bazą danych odbywa się w ramach usługi Virtual network. Poszczególne usługi korzystają z komponentów opartych o platformę Azure oraz jej komponenty bazodanowe pod Postgresql.

System wykorzystuje infrastrukturę Azure w celu przechowywania plików graficznych oraz przesyłania danych służących do monitorowania zachowania aplikacji. Aktualizacja danych z podstawowych, produkcyjnych baz danych Systemu RATUSZ prowadzona jest na dwa sposoby: ręcznie wprowadzone zmiany w harmonogramie wywozu odpadów w panelu administratora lub poprzez zaimportowanie pliku xlsx z gotowym harmonogramem wywozu odpadów w panelu administratora.

4 Załącznik nr 2 - Warunki dostępu zdalnego do Infrastruktury Teleinformatycznej Zamawiającego, w tym dostępne dla zasoby

4.1 Zasoby Infrastruktury Teleinformatycznej dostępne dla Pentestera

1. Celem wykonania zamówienia Zamawiający zapewni Pentesterowi do przeprowadzenia testów bezpieczeństwa po stronie infrastruktury wewnętrznej niezbędne zasoby techniczne w formie maszyn wirtualnych opartych o techniczne zasoby:
    1.1. serwerów fizycznych do wirtualizacji Huawei Fusion 1288H (dwie maszyny dwuprocesorowe): dostępne wolne zasoby: liczba rdzeni: 4, pamięć RAM: 64 GB;
    1.2. macierzy dyskowej „Metro Storage Cluster" (MSC) zbudowanej przez dwie macierze Huawei Ocean Dorado 3000: pojemność dostępna dla Pentestera: do 2TB;
    1.3. oprogramowania systemowego: dwie licencje MS Windows Data Center Server 2021 wraz z licencjami CAL oraz oprogramowanie do wirtualizacji Hyper-V.
2. Zamawiający nie ogranicza Pentestera w zdefiniowaniu niezbędnych środowisk uruchomieniowych (VM) do przeprowadzenia testów, jednak musi to mieć swoje racjonalne uzasadnienie np. w wytycznych producentów oprogramowania użytego do realizacji zamówienia.
3. Zabezpieczenie kopii maszyn wirtualnych użytych do realizacji zamówienia leży po stronie Zamawiającego, który posiada do tego niezbędne zasoby oraz licencje oprogramowania: NAKIVO Backup & Replication. Licencje te posłużą do utworzenia i utrzymywania kopii bezpieczeństwa środowiska produkcyjnego Systemu RATUSZ (tj. kopii obrazów maszyn wirtualnych poddawanych testom bezpieczeństwa).

4.2 Wymagania dot. instalacji, administrowania maszynami wirtualnymi

1. Zakres zobowiązań Pentestera obejmuje wszelkie czynności dot. instalacji oraz konfiguracji wykorzystywanego do realizacji zamówienia Oprogramowania np. pakietu Kali – Linux. Z tego zakresu zobowiązań Pentestera Zamawiający wyłącza czynności podstawowej konfiguracji maszyn wirtualnych (VM), jakie będą niezbędne do realizacji zamówienia.
2. W związku z powyższym parametry każdej maszyny wirtualnej (VM) muszą być opisane przez Wykonawcę oraz przekazane Zamawiającemu drogą elektroniczną, zgodnie z przyjętymi zasadami komunikacji.
3. Podobne ograniczenia występują w czynnościach administrowania, gdzie administrowanie maszynami wirtualnymi jest wyłącznie w gestii Zamawiającego, a czynności zarządzania konfiguracją na poziomie systemowym, narzędziowym, bazodanowym, aplikacyjnym (o ile jest niezbędne) leży po stronie zobowiązań Pentestera.
4. W każdym przypadku, kiedy niezbędne będzie podjęcie czynności związanych z administrowaniem lub konfiguracją maszyny wirtualnej, Pentester jest zobowiązany skontaktować się z Zamawiającym, który te czynności wykonywać będzie bez zbędnej zwłoki.

5. Zasady współdziałania Pentestera i Zamawiającego w zakresie wskazanym powyżej powinny być uszczegółowione i uzgodnione przez Strony na etapie przygotowania realizacji zamówienia przez obustronne uzgodnienie zasad komunikacji.

6. Zakres zobowiązań Zamawiającego nie może wykraczać poza zakres zobowiązań określony w niniejszej specyfikacji oraz w projekcie umowy.

4.3 Zasady zdalnego dostępu do Infrastruktury Teleinformatycznej

1. Zamawiający zapewni dla Pentestera zdalny dostęp do jego Infrastruktury Teleinformatycznej (Infrastruktury Technicznej) celem realizacji przez niego przedmiotu zamówienia pod następującymi warunkami:

   1.1. Dostęp dla Pentestera możliwy będzie wyłącznie po podpisaniu przez Wykonawcę oświadczenia o zapewnieniu podczas realizacji zamówienia zasad określonych przez obowiązującą w organizacji Zamawiającego Politykę Bezpieczeństwa Informacji (PBI) lub dokumenty stanowiące projektowany System Zarządzania Bezpieczeństwem Informacji (SZBI), przy uwzględnieniu, iż:

      1.1.1. Zdalny dostęp do Infrastruktury Technicznej będzie wyłącznie możliwy poprzez łącze VPN udostępnionego przez Zamawiającego klienta oprogramowania VPN;

      1.1.2. Dostęp posiadać będzie wyłącznie określona liczba osób wskazana przez Wykonawcę w przekazanym i zaakceptowanym przez Zamawiającego wykazie osób: /imię/nazwisko/e-mail/tel/firma – o ile jest to podwykonawca;

      1.1.3. Dostęp będzie realizowany na żądanie lub w trybie określonym przez harmonogram ustalonych „okien czasowych” na prowadzone prace;

      1.1.4. Dostęp do zasobów będzie realizowany przez VPN poprzez konta imienne aktywowane w oparciu o harmonogram prowadzenia prac w zakresie testowania Systemu.

2. Naruszenie przez Wykonawcę przyjętych powyższych zasad może skutkować stałym lub czasowym zablokowaniem dostępu zdalnego.

5 Załącznik nr 3 – Wybrane pojęcia, definicje

Nazwa	Definicja
Analiza ryzyka (systemu teleinformatycznego)	Analiza i ocena – zagrożeń, zdarzeń polegających na wykorzystaniu lub zaistnieniu podatności systemu teleinformatycznego przetwarzającego dane.
Anonimizacja	Przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo, jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań (art. 3 pkt 1 ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, Dz. U. 2020 Nr 158 t.j.) . Anonimizacja pozwala na trwałe (nieodwracalne) usunięcie powiązań między danymi osobowymi, a osobą, której dotyczą. W ten sposób informacje, które były danymi osobowymi, przestają nimi być (odwrotność pseudonimizacji).
API	API (ang. Application Programming Interface, interfejs programowania aplikacji) – ściśle określony zestaw reguł i ich opisów, w jaki programy komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych. Elementem API jest dokumentacja techniczna umożliwiająca jego wykorzystanie przez zewnętrzne systemy.
Aplikacja	Wydzielona część systemu przetwarzającego dane realizująca cel biznesowy, zapewniająca ustalony zakres funkcjonalny dla użytkownika.
Audyt	Systematyczna i niezależna ocena danej organizacji, systemu, procesu, projektu lub produktu. Audyt dzielimy ze względu na osobę/podmiot wykonującą/y – na wewnętrzny lub zewnętrzny.
Audyt bezpieczeństwa systemu teleinformatycznego	Niezależny przegląd i ocena systemu przetwarzania danych w celu weryfikacji, przetestowania adekwatności zastosowanych środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką bezpieczeństwa, procedurami operacyjnymi, w tym dokumentacją systemu w celu wykrycia przełamań bezpieczeństwa i wydania zaleceń dotyczących środków nadzorowania oraz polityki bezpieczeństwa.
Baza danych	Zbiór powiązanych ze sobą logicznie danych, zaprojektowany dla zaspokojenia potrzeb informacyjnych organizacji w określonym zakresie dziedzinowym objętym funkcjonowaniem dziedzinowego systemu teleinformatycznego.
Dokument elektroniczny	Zgodnie z definicją zawartą w Art. 3 pkt. 2) Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 670z późn. zm.), inaczej Uoinf– stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.
Elektroniczna usługa publiczna, inaczej e-usługa	Na podstawie dyrektywy 77/388/EWG z 2005 roku art. 9 ust. 2 lit. e) / załącznik L dyrektywy: Usługa, która jest świadczona drogą elektroniczną za pomocą sieci Internet, której wykonanie z jednej strony jest w określonym zakresie zautomatyzowane i wymaga tylko niewielkiego udziału człowieka, (jako usługobiorcy), a z drugiej strony w takim zakresie, w jakim jest świadczone –

Nazwa	Definicja
	wykonanie jej bez technologii informatycznej jest niemożliwe.
Formularz elektroniczny	Uoinf Art. 3 pkt. 25) formularz elektroniczny – graficzny interfejs użytkownika wystawiany przez oprogramowanie, służący do przygotowania i wygenerowania dokumentu elektronicznego zgodnego z odpowiadającym mu wzorem dokumentu elektronicznego.
Platforma (portal) e-urząd	Aplikacja sieciowa w formie portalu internetowego z interfejsem umożliwiającym dostęp do wybranych danych z rejestrów publicznych, w tym danych z ewidencji i rejestrów podatkowych oraz opłat za pośrednictwem przeglądarki internetowej.
Iteracja	Wielokrotne, policzalne powtórzenie jednostki zachowania w ramach określonych czynności.
Infrastruktura Techniczna Zamawiającego	Sprzęt komputerowy (serwery, macierze, urządzenia aktywne i pasywne oraz pozostałe elementy instalacyjno – konfiguracyjne infrastruktury teleinformatycznej) jak również Oprogramowanie: Aplikacyjne, Systemowe, Narzędziowe, Bazodanowe, stanowiące środowisko uruchomieniowe wdrażanego Systemu RATUSZ
Inwazyjny atak	Symulacja rzeczywistego ataku, którego rezultatem jest np. utrata integralności danych, spowodowanie błędnego działania Systemu lub wyłączenie określonych jego funkcji, usług, pozyskanie danych - wypływ wrażliwość danych i / lub ich modyfikacja, zainstalowanie, uruchomienie wirusa, zaszyfrowanie danych – i inne. Atak może być uzupełniony zatarciem śladów ataku.
Komponent	Hermetyczny moduł lub część oprogramowania systemu informatycznego przetwarzającego dane, realizujący usługi za pośrednictwem interfejsów.
Krajowe Ramy Interoperacyjności (KRI)	Zbiór uzgodnionych definicji, wymagań, reguł architektury systemów teleinformatycznych oraz procedur i zasad, których stosowanie umożliwi współdziałanie systemów teleinformatycznych podmiotów realizujących zadania publiczne w procesach realizacji tych zadań drogą elektroniczną.
Metodyka	Zestaw pojęć, notacji, modeli formalnych, języków i sposobów postępowania służący do analizy rzeczywistości (stanowiącej przedmiot projektowanego systemu informatycznego) oraz do projektowania pojęciowego, logicznego i/lub fizycznego. Zwykle metodyka jest powiązana z odpowiednią notacją (diagramami) służącymi do zapisywania wyniku poszczególnych faz projektu, jako środek wspomagający ludzką pamięć i wyobraźnię, a także jako środek komunikacji w zespołach oraz pomiędzy projektantami i klientem.
Moduł (Aplikacja)	Część Systemu realizująca określoną, logiczną całość funkcji w ramach infrastruktury aplikacyjnej.
Naruszenie ochrony danych osobowych	Na podstawie art. 4 pkt 12) RODO – naruszenie ochrony / bezpieczeństwa danych osobowych to - przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie lub nieuprawnione ujawnienie lub nieuprawniony dostęp do zgromadzonych lub przesyłanych lub w inny sposób przetwarzanych danych osobowych.
Norma (specyfikacja techniczna)	Dokument przyjęty na zasadzie konsensusu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub zmierzający do określenia i uzyskania optymalnego stopnia uporządkowania w określonym zakresie.
Oprogramowanie	Oprogramowanie Aplikacyjne, Standardowe, Bazodanowe, Narzędziowe oraz

Nazwa	Definicja
	Systemowe, rozumiane łącznie jak również każde z nich z osobna zależnie od kontekstu wystąpienia.
Oprogramowanie Aplikacyjne	Oprogramowanie opracowane i dostarczone przez wykonawcę, stanowiące najwyższą warstwę w wielowarstwowej architekturze budowanego Systemu, do którego tenże posiada autorskie prawa majątkowe. Oprogramowanie Aplikacyjne obejmuje wszystkie opracowane przez tego Wykonawcę komponenty, procedury mające jakąkolwiek postać kodu wykonywalnego lub skryptu użytego do uruchomienia i funkcjonowania Systemu.
Oprogramowanie Standardowe	Oprogramowanie wykonawcy, co do którego tenże posiada autorskie prawa majątkowe lub prawa takie należą do osoby trzeciej. Oprogramowanie to zostało wytworzone przed udzieleniem wykonawcy zamówienia i stanowi zamkniętą całość w formie modułu / komponentu / biblioteki programistycznej oraz służyć będzie do budowy i Wdrożenia Systemu.
Oprogramowanie Bazodanowe	Oprogramowanie zapewniające techniczne środki do bezpiecznego gromadzenia oraz autoryzowanego dostępu i przetwarzania danych w oparciu o relacyjną, obiektową lub obiektowo – relacyjną bazę danych.
Oprogramowanie Narzędziowe	Oprogramowanie zapewniające niezbędne funkcje techniczne na rzecz budowy i Wdrożenia Systemu, stanowiące warstwę pośrednią - usługową pomiędzy Oprogramowaniem Aplikacyjnym / Standardowym a Systemowym, z wyłączeniem Oprogramowania Bazodanowego.
Oprogramowanie Systemowe	Oprogramowanie zapewniające podstawowe funkcje systemowe umożliwiające funkcjonowanie infrastruktury sprzętowej zgodnie z jej przeznaczeniem. W skład tego oprogramowania wchodzą: oprogramowanie do wirtualizacji oraz systemy operacyjne.
Podatność	Słabość lub luka w systemie przetwarzania danych. Wady lub luki w strukturze fizycznej, organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone i niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika
Przypadek użycia	Opis wymagań wobec systemu teleinformatycznego przedstawiający interakcję pomiędzy „aktorem", który inicjuje zdarzenie oraz opisywanym systemem – zdefiniowany przez opis sekwencji prostych kroków. Przypadek użycia może być przedstawiony graficznie w formie tzw. diagramu przypadków użycia. Uogólniając przypadek użycia może odnosić się do zachowania obiektu w pewnym działaniu zmierzającym do osiągnięcia określonego stanu.
Przypadek testowy	Ściśle określona „ścieżka przejścia" w ramach procedury testowej prowadzonej zgodnie z planem testów odnosząca się do określonego scenariusza zachowania testowanego produktu lub charakterystycznej klasy danych wejściowych. Kluczowe dla właściwego określenia przypadku testowego jest jednoznaczne określenie oczekiwanego, spodziewanego wyniku wykonania procedury testowej.
Pseudonimizacja	Przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (RODO). Zalecane techniki pseudonimizacji zawarte w opinii 05/2014 wydanej przez Grupę Roboczą ds. ochrony osób

Nazwa	Definicja
	fizycznych w zakresie przetwarzania danych osobowych (RODO Art. 29) to: szyfrowanie z kluczem; funkcje hash tzw. funkcje skrótu, zastosowanie tokena.
RODO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE – tzw. ogólne rozporządzenie o ochronie danych.
Rejestr publiczny	Uoinf Art. 3 pkt. 5) rejestr publiczny – rejestr, ewidencja, wykaz, lista, spis albo inna forma ewidencji, służące do realizacji zadań publicznych, prowadzone przez podmiot publiczny na podstawie odrębnych przepisów ustawowych.
Schemat aplikacyjny	Schemat pojęciowy dla danych wykorzystywanych przez jedną lub więcej aplikacji.
System	W skrócie system teleinformatyczny RATUSZ wdrażany w organizacji Zamawiającego
System teleinformatyczny	Uoinf Art. 3 pkt. 3) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r., poz.576 t.j.).
Testy bezpieczeństwa	Testy sprawdzające podatność oraz poprawność i skuteczność funkcjonowania zabezpieczeń oprogramowania. Zabezpieczenia są to środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko. Zakres działania Pentestera w obszarze testów może obejmować również działania socjotechniczne.
Testy funkcjonalne	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie wymagań funkcjonalnych testowanego oprogramowania.
Testy integracyjne – komunikacji	Testy poprawności powiązań między modułami / usługami oraz systemami zewnętrznymi
Testy niefunkcjonalne	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie parametrów i cech niefunkcjonalnych testowanego oprogramowania.
Testy penetracyjne	Testy polegające na autoryzowanej „siłowej” próbie oceny bezpieczeństwa infrastruktury teleinformatycznej. Testy penetracyjne można nazwać etycznym hackingiem.
Testy regresyjne	Testy regresyjne, inaczej retesty są to testy sprawdzające, czy określona funkcjonalność lub rozwiązania w zabezpieczeń zostały doprowadzone do zgodności technicznej i zapewniają wymagane cechy funkcjonalne oraz ustalony poziom bezpieczeństwa dla danego komponentu programistycznego.
Testy wydajnościowe	Testy sprawdzające zgodność ze specyfikacją lub dokumentacją techniczną w zakresie parametrów wydajnościowych systemu lub jego części – stanowią część testów akceptacyjnych lub weryfikacyjnych prowadzonych przez podmiot trzeci.
Testy black box	Rodzaj testów. Testy te zakładają, że jest znana specyfikacja systemu natomiast nie jest znana znajomość konstrukcji architektury systemu. Podczas testów system jest traktowany jak czarna skrzynka. Testy są symulacją zewnętrznego ataku.

Nazwa	Definicja
Testy grey box / gray box	Rodzaj testów. Testy te zakładają, iż znana jest częściowo lub w całości specyfikacja systemu dot. architektury systemu oraz przyjętych rozwiązań technologicznych, w tym zastosowanych produktów. Testy mogą być symulacją zewnętrznego ataku oraz są mogą być ukierunkowane na ocenę zabezpieczeń wnętrza systemu. Użycie nazwy „gray box" (zwrot w języku amerykańskim) ma swoje praktyczne, zwyczajowe użycie w języku branżowym – obie nazwy dla tego rodzaju testów są sobie równoważne.
Usługi (publiczne)	Usługi świadczone przez organy administracji publicznej dla obywateli, podmiotów gospodarczych oraz organizacji, a także inne formy komunikacji pomiędzy organami administracji publicznej a obywatelami i organizacjami, służące realizacji zadań administracji publicznej lub wywiązywaniu się obywateli i organizacji z obowiązków wobec państwa
Usługa sieciowa	Komponent / część oprogramowania, realizujący określone funkcje logiki Systemu. Komponent może być wywołany zdalnie poprzez zdefiniowany interfejs.
Wzór dokumentu elektronicznego	Uoinf Art. 3 pkt. 24) wzór dokumentu elektronicznego – zbiór danych określających zestaw, sposób oznaczania oraz wymagalność elementów treści i metadanych dokumentu elektronicznego, a także mogących określać sposób zapisu danych dla wskazanych elementów oraz kolejność i sposób wyświetlania na ekranie lub drukowania poszczególnych elementów (wizualizacji).

6 Załącznik nr 4 – Aplikacja Web – Platforma (portal) e-Urząd

Treść załącznika zawiera odrębny, zewnętrzny dokument będący integralną częścią OPZ o nazwie: Załącznik nr 4 – Aplikacja Web – Platforma (portal) e-Urząd