

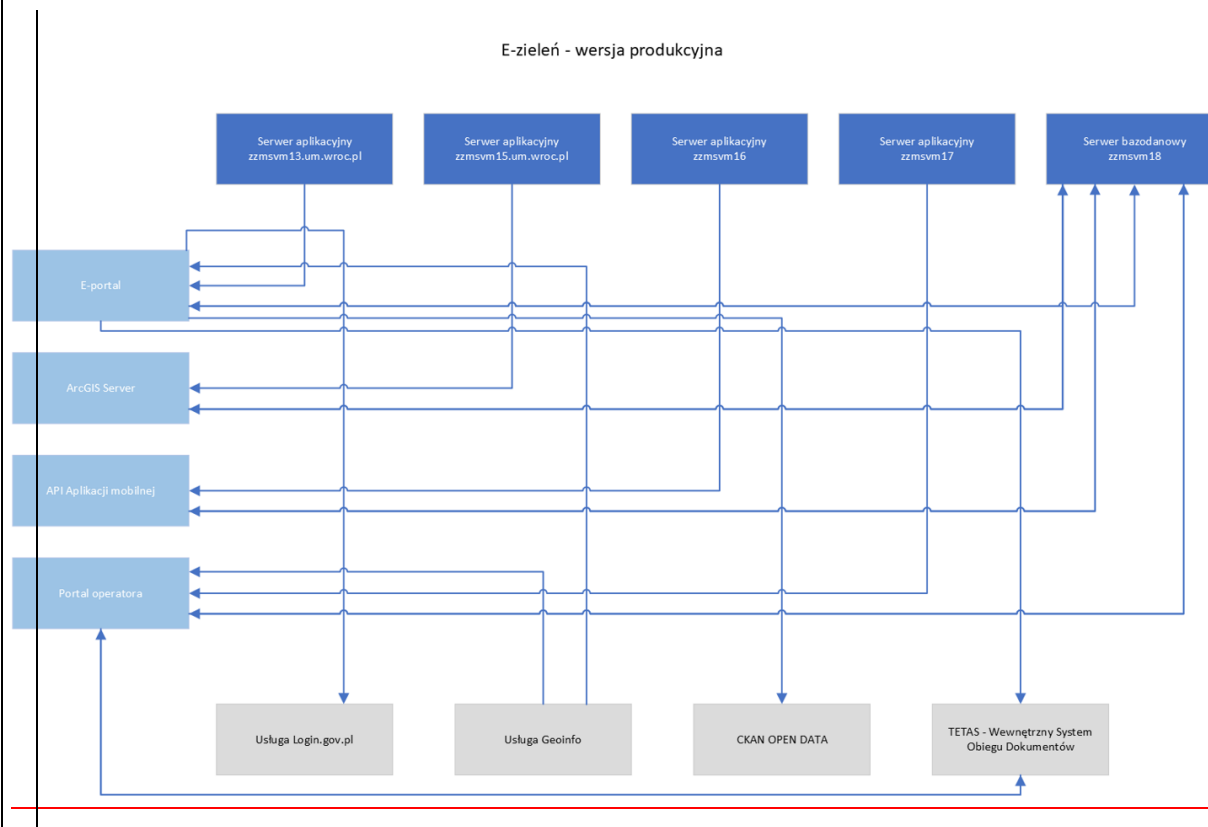
Przedmiot zamówienia.

System 1

Audyty bezpieczeństwa i re-audyty.

1. System Informatyczny 1 składający się z 2 aplikacji www oraz 1 aplikacji mobilnej.

Schemat blokowy systemu:



1. Zamawiający ma prawo do zlecenia audytu bezpieczeństwa Systemu firmie zewnętrznej zgodnie z ustalonym harmonogramem. Termin ten nie może być dłuższy niż 60 dni od dnia poinformowania Usługodawcy.
2. Audyt będzie przeprowadzony przez firmę zewnętrzną z zachowaniem pełnej współpracy na styku Zamawiający-Wykonawca-Usługodawca.
3. Usługodawca nie może odmówić przeprowadzenia audytu bezpieczeństwa Systemu.
4. Audytowi bezpieczeństwa podlegać będą wszystkie elementy składające się na całość rozwiązania Systemu tj. serwery aplikacyjne, bazy danych, moduły wewnętrzne aplikacji, aplikacje klienckie i mobilne.

Zakres prac związanych z audytem bezpieczeństwa obejmuje:

I. Weryfikacja realizacji przez Wykonawcę systemu wymogów bezpieczeństwa oraz zgodności z przepisami prawa, wskazanych w OPZ na zakup systemu.

II. Weryfikacja bezpieczeństwa elementów architektury audytowanego systemu, w tym bezpieczeństwo punktów styku Systemu z wewnętrznymi i zewnętrznymi serwisami, bazami danych oraz serwisami centralnymi (np. Węzeł Identyfikacji Elektronicznej, ePUAP, etc.)

III. Standardowe czynności związane z audytem bezpieczeństwa aplikacji:

1. Przeprowadzenie testów penetracyjnych typu blackbox i greybox,
2. Badanie aplikacji pod kątem odporności na ataki w zakresie:
 - autoryzacji, uwierzytelniania i kontroli dostępu,
 - zarządzania sesją,
 - walidacji wejścia,
 - mechanizmów kryptograficznych oraz danych wrażliwych,
 - konfiguracji systemu,
 - logowania,
3. Analizę podatności i zagrożeń,
4. Badanie bezpieczeństwa API, w tym identyfikacja luk w autoryzacji, manipulacje danymi, itp.
5. Analizę konfiguracji (serwery, systemy operacyjne, bazy danych, usługi, porty),
6. Podczas testów szukane będą podatności w oparciu o OWASP TOP 10:
 - A01. Błędy kontroli dostępu- (Broken Access Control)
 - A02. Błędy kryptograficzne- (Cryptographic Failures)
 - A03. Wstrzyknięcie- (Injection)
 - A04. Niepewna konstrukcja- (Insecure Design)
 - A05. Błędna konfiguracja zabezpieczeń- (Security Misconfiguration)
 - A06. Wrażliwe i podatne komponenty- (Vulnerable and Outdated Components)
 - A07. Błędy w identyfikacji i uwierzytelnianiu- (Identification and Authentication Failures)
 - A08. Błędy oprogramowania i integralności danych- (Software and Data Integrity Failures).
 - A09. Awarie logowania i monitorowania bezpieczeństwa- (Security Loggin and Monitoring Failures)
 - A10. Fałszowanie żądań po stronie serwera- (Server-Side Request Forgery (SSRF))
7. Dodatkowo powinny być analizowane takie elementy aplikacji webowych jak:
 - Nagłówki wysyłane przez serwer
 - Pliki cookie
 - Skrypty javascript
 - Elementy RIA aplikacji webowych (pliki SWF, aplety java)

- Czasy odpowiedzi serwera przy poszczególnych operacjach
- Reakcja na dane wejściowe w zapytaniach (nagłówki, agent przeglądarki, wadliwe zapytania protokołu HTTP)
- Próby aplikacyjnych ataków DoS
- Mechanizm HTTP Strict Transport Security
- Aktualność wtyczek i bibliotek
- Enumeracje haseł i loginów
- XSS (Skrypty między witrynami)

Testy zakładają również badanie pod kątem bezpieczeństwa zachowania logiki aplikacji. W tej części testów osoby audytujące utworzą szereg scenariuszów, które następnie będą przetestowane. Scenariusze są opracowywane pod kątem logiki działania danego systemu.

Dodatkowo przeprowadzone testy będą symulowały próby przeprowadzenia ataków na aplikację z strony:

- Użytkownika niezalogowanego
- Klienta aplikacji

8. Prace powinny być wykonywane z uwzględnieniem najlepszych praktyk oraz metodyk takich jak OSSTMM v3, ISSAF oraz OWASP TOP 10 oraz tych dotyczących aplikacji desktopowych i mobilnych.

9. Jeśli komponenty aplikacji występują również w wersji mobilnej należy również przeprowadzić testy w oparciu o OWASP MAS zawierający między innymi OWASP MASVS oraz OWASP MASTG :

- MASVS-STORAGE: Bezpieczne przechowywanie poufnych danych na urządzeniu (dane w spoczynku).
- MASVS-CRYPTO: Funkcja kryptograficzna używana do ochrony poufnych danych.
- MASVS-AUTH: Mechanizmy uwierzytelniania i autoryzacji używane przez aplikację mobilną.
- MASVS-NETWORK: Bezpieczna komunikacja sieciowa między aplikacją mobilną a zdalnymi punktami końcowymi (dane w tranzycie).
- MASVS-PLATFORM: Bezpieczna interakcja z bazową platformą mobilną i innymi zainstalowanymi aplikacjami.
- MASVS-CODE: Najlepsze praktyki w zakresie bezpieczeństwa przetwarzania danych i aktualizacji aplikacji.
- MASVS-RESILIENCE: Odporność na inżynierię wsteczną i próby manipulacji.

W celu uzupełnienia OWASP MASVS, należy posiłkować się OWASP MASTG oraz OWASP MAS Checklist, jako uzupełnienie testów bezpieczeństwa aplikacji mobilnych.

10. Audyt zgodności z obowiązującymi przepisami bezpieczeństwa danych osobowych i Polityk Bezpieczeństwa Zamawiającego.

Zakres obejmuje:

- sprawdzenie zgodności Systemu pod kątem obowiązujących rozporządzeń Parlamentu Europejskiego i Rady nr 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (inaczej ogólne rozporządzenie o ochronie danych osobowych - RODO),
- sprawdzenie Wykonawcy systemu i spełnienia przez niego zasad RODO poprzez uzyskanie odpowiedzi, od Wykonawcy systemu, na pytania zawarte w ankiecie (pytania są zbiorem minimalnym, mogą być rozszerzone przez Audytora) oraz sprawdzenie procedur dotyczących ochrony danych u Wykonawcy systemu i ich zgodności z wybranymi zapisami Polityki Ochrony Danych i Bezpieczeństwa Informacji wskazanymi przez Zamawiającego.

L.P. PYTANIE, TAK/NIE, DODATKOWE WYJAŚNIENIA, WIEDZA FACHOWA

1. Czy podmiot przetwarzający posiada doświadczenie w świadczeniu usług związanych z powierzeniem przetwarzania danych? Jeśli tak, to jak długie? Czy udokumentowane?
2. Czy przepisy prawa wymagają, aby dany podmiot przetwarzający wyznaczył IOD?
3. Czy dany podmiot przetwarzający wyznaczył IOD?

(Jeśli tak, proszę o przekazanie informacji kontaktowych do IOD)

4. Czy podmiot przetwarzający wyznaczył inną osobę/zespół odpowiedzialny za nadzór nad ochroną danych osobowych w organizacji?
5. Czy osoby po stronie podmiotu przetwarzającego dedykowane do obsługi administratora danych zostały przeszkolone i zapoznane z przepisami o ochronie danych? Czy jest to udokumentowane?
6. Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie obsługi, w tym bezpiecznego korzystania z systemu informatycznego, jeżeli jest on stosowany do przetwarzania danych przez podmiot przetwarzający?
7. Czy osoby zatrudnione w podmiocie przetwarzającym przy przetwarzaniu danych zostały przeszkolone w zakresie zasad bezpieczeństwa informacji?

WIARYGODNOŚĆ

8. Czy podmiot przetwarzający posiada referencje od innych podmiotów, które obsługuje/obsługiwał w zakresie przetwarzania danych osobowych na ich zlecenie? Jeśli tak, czy można się z nią zapoznać?
9. Czy stwierdzono prawomocną decyzją UODO/innego organu nadzorczego lub prawomocnym wyrokiem sądu naruszenie ochrony danych osobowych przez podmiot przetwarzający?
10. Czy podmiot przetwarzający stosuje się do przyjętych przez organ nadzorczy kodeksów postępowania?
11. Czy podmiot przetwarzający objęty jest monitorowaniem przestrzegania kodeksu postępowania przez akredytowany podmiot monitorujący?
12. Czy podmiot przetwarzający otrzymał certyfikat zgodności z RODO?

13. Kryterium wewnętrzne: Czy rozważany podmiot jest znany na rynku jako podmiot wykonujący danego rodzaju usługi? Jeżeli tak, jaką ma renomę? Jakie są opinie o tym podmiocie, o współpracy z tym podmiotem, o stosowanych przez niego zabezpieczeniach czy przetwarzaniu danych?

ZASOBY

14. Czy podmiot przetwarzający opracował i wdrożył politykę ochrony danych lub podobną procedurę? Jeśli tak, prosimy o jej przedstawienie.

15. Czy podmiot przetwarzających wdrożył procedurę/instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych?

16. Czy podmiot przetwarzający prowadzi ewidencję naruszeń przepisów o ochronie danych osobowych, w tym naruszeń bezpieczeństwa danych?

17. Czy podmiot przetwarzający prowadzi rejestr przetwarzanych zbiorów danych osobowych lub zasobów informacyjnych?

18. Czy podmiot przetwarzający prowadzi rejestry czynności przetwarzania danych osobowych (jako ADO oraz jako procesor)?

19. Czy podmiot przetwarzający wdrożył zasady zarządzania bezpieczeństwem informacji, w tym:

19a. system zarządzania bezpieczeństwem informacji na podstawie normy ISO 27001? Czy posiada certyfikat?

19b. zasady zarządzania bezpieczeństwem informacji z elementami wykorzystania normy ISO 27002?

19c. zasady zarządzania bezpieczeństwem informacji zgodne z wymaganiami Krajowych Ram Interoperacyjności?

20. Czy podmiot wdrożył inne zasady ochrony informacji – (np. Polityka bezpieczeństwa informacji, Polityki ochrony danych osobowych, które są jego wewnętrznymi regulacjami)?

20a. Czy podmiot wdrożył inne zasady ochrony informacji –

(Ramy prywatności, Praktyczne zasady ochrony informacji o identyfikowalnych osobach, Wytyczne dotyczące oceny skutków dla prywatności, itp.)?

20b. Czy podmiot wdrożył inne zasady, standardy, regulaminy, procedury, polityki, biblioteki lub zbiory najlepszych praktyk mające znaczenie dla ochrony informacji/danych osobowych?

21. Czy podmiot przetwarzający dobrał zabezpieczenia zapewniające bezpieczeństwo przetwarzanych danych osobowych w odniesieniu do oceny skutków ich przetwarzania dla praw i wolności osób, których dane dotyczą? (na podstawie szacowania ryzyka pod kątem ochrony prywatności - DPIA)?

22. Czy szacowanie ryzyka zostało udokumentowane, np. czy został stworzony plan postępowania z ryzykiem lub zakres zastosowania?

23. Czy podmiot przetwarzający okresowo przeprowadza kolejne działania związane z szacowaniem ryzyka pod kątem ochrony prywatności? Czy w przypadku zmiany poziomu ryzyka dobiera nowe środki techniczne i organizacyjne zabezpieczające dane, stosownie do wyników analizy?

24. Czy podmiot przetwarzający wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z ich przetwarzaniem, w tym:

a) pseudonimizację i szyfrowanie danych,

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

25. Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania?

26. Czy wnioski z audytów zostały udokumentowane, np. w raporcie audytowym?

27. Czy podmiot przetwarzający jest przygotowany do poddania się audytowi przeprowadzonemu przez administratora danych lub audytora upoważnionego przez administratora danych?

28. Czy osoby delegowane do obsługi ADO posiadają nadane upoważnienia do przetwarzania danych? Czy zostało to udokumentowane? Prosimy o przedłożenie listy osób upoważnionych, które będą obsługiwać ADO.

29. Czy osoby upoważnione do przetwarzania danych w ramach obsługi ADO zostały obowiązane do zachowania ich w tajemnicy? Czy zostało to udokumentowane?

30. Czy podmiot przetwarzający wprowadził procedurę upoważniania osób uczestniczących w przetwarzaniu danych osobowych do ich przetwarzania?

Oświadczam, że wszystkie informacje zawarte w niniejszej ankiecie są zgodne z prawdą.

Data i podpisy osób upoważnionych do reprezentacji podmiotu zgodnie z KRS

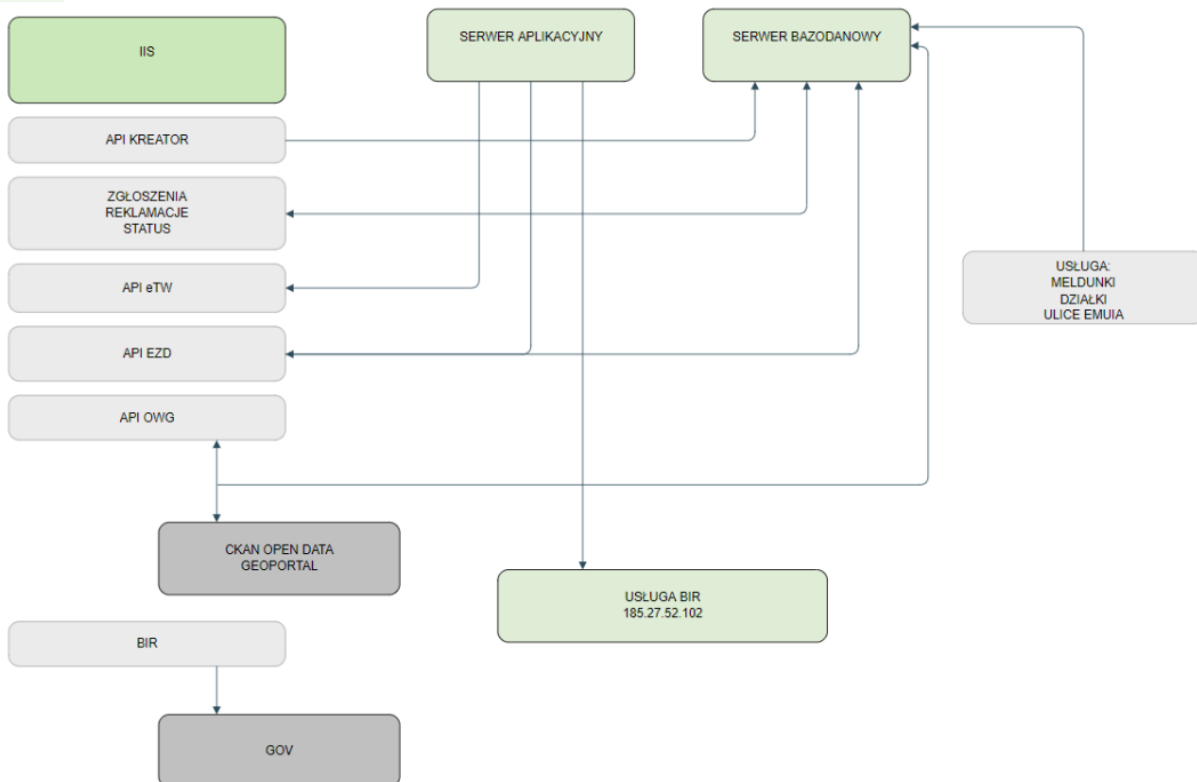
Przedmiot zamówienia.

System 2

Audyt bezpieczeństwa i re-audyt.

1. System Informatyczny 2 składającego się z 4 aplikacji www oraz 2 aplikacji desktopowych zgodnie z załączonym OPZ.

Schemat blokowy systemu:



1. Zamawiający ma prawo do zlecenia audytu bezpieczeństwa Systemu firmie zewnętrznej zgodnie z ustalonym harmonogramem. Termin ten nie może być dłuższy niż 60 dni od dnia poinformowania Usługodawcy.
2. Audyt będzie przeprowadzony przez firmę zewnętrzną z zachowaniem pełnej współpracy na styku Zamawiający-Wykonawca-USługodawca.
3. Usługodawca nie może odmówić przeprowadzenia audytu bezpieczeństwa Systemu.
4. Audytowi bezpieczeństwa podlegać będą wszystkie elementy składające się na całość rozwiązania Systemu tj. serwery aplikacyjne, bazy danych, moduły wewnętrzne aplikacji, aplikacje klienckie i mobilne.

Zakres prac związanych z audytem bezpieczeństwa obejmuje:

I. Weryfikacja realizacji przez Wykonawcę systemu wymogów bezpieczeństwa oraz zgodności z przepisami prawa, wskazanych w OPZ na zakup systemu.

II. Weryfikacja bezpieczeństwa elementów architektury audytowanego systemu, w tym bezpieczeństwo punktów styku Systemu z wewnętrznymi i zewnętrznymi serwisami, bazami danych oraz serwisami centralnymi (np. Węzeł Identyfikacji Elektronicznej, ePUAP, etc.)

III. Standardowe czynności związane z audytem bezpieczeństwa aplikacji:

1. Przeprowadzenie testów penetracyjnych typu blackbox i greybox,
2. Badanie aplikacji pod kątem odporności na ataki w zakresie:
 - autoryzacji, uwierzytelniania i kontroli dostępu,
 - zarządzania sesją,
 - walidacji wejścia,
 - mechanizmów kryptograficznych oraz danych wrażliwych,
 - konfiguracji systemu,
 - logowania,
3. Analizę podatności i zagrożeń,
4. Badanie bezpieczeństwa API, w tym identyfikacja luk w autoryzacji, manipulacje danymi, itp.
5. Analizę konfiguracji (serwery, systemy operacyjne, bazy danych, usługi, porty),
6. Podczas testów szukane będą podatności w oparciu o OWASP TOP 10:
 - A01. Błędy kontroli dostępu- (Broken Access Control)
 - A02. Błędy kryptograficzne- (Cryptographic Failures)
 - A03. Wstrzyknięcie- (Injection)
 - A04. Niepewna konstrukcja- (Insecure Design)
 - A05. Błędna konfiguracja zabezpieczeń- (Security Misconfiguration)
 - A06. Wrażliwe i podatne komponenty- (Vulnerable and Outdated Components)
 - A07. Błędy w identyfikacji i uwierzytelnianiu- (Identification and Authentication Failures)
 - A08. Błędy oprogramowania i integralności danych- (Software and Data Integrity Failures).
 - A09. Awarie logowania i monitorowania bezpieczeństwa- (Security Loggin and Monitoring Failures)
 - A10. Fałszowanie żądań po stronie serwera- (Server-Side Request Forgery (SSRF))
7. Dodatkowo powinny być analizowane takie elementy aplikacji webowych jak:
 - Nagłówki wysyłane przez serwer
 - Pliki cookie

- Skrypty javascript
- Elementy RIA aplikacji webowych (pliki SWF, aplety java)
- Czasy odpowiedzi serwera przy poszczególnych operacjach
- Reakcja na dane wejściowe w zapytaniach (nagłówki, agent przeglądarki, wadliwe zapytania protokołu HTTP)
- Próby aplikacyjnych ataków DoS
- Mechanizm HTTP Strict Transport Security
- Aktualność wtyczek i bibliotek
- Enumeracje haseł i loginów
- XSS (Skrypty między witrynami)

Testy zakładają również badanie pod kątem bezpieczeństwa zachowania logiki aplikacji. W tej części testów osoby audytujące utworzą szereg scenariuszów, które następnie będą przetestowane. Scenariusze są opracowywane pod kątem logiki działania danego systemu.

Dodatkowo przeprowadzone testy będą symulowały próby przeprowadzenia ataków na aplikację z strony:

- Użytkownika niezalogowanego
- Klienta aplikacji

8. Prace powinny być wykonywane z uwzględnieniem najlepszych praktyk oraz metodyk takich jak OSSTMM v3, ISSAF oraz OWASP TOP 10 oraz tych dotyczących aplikacji desktopowych i mobilnych.