



Załącznik nr 1 do umowy

Szczegółowy opis przedmiotu zamówienia

Audyt bezpieczeństwa systemu informacyjnego dla podmiotu publicznego jako kluczowego w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa oraz wypełnienie końcowej ankiety dojrzałości cyberbezpieczeństwa

1. Podstawowe założenia audytu

Przeprowadzony audyt zweryfikuje system zarządzania bezpieczeństwem informacji u Zamawiającego obejmując ocenę architektury teleinformatycznej, konfiguracji systemów, mechanizmów ochrony oraz procesów zarządzania bezpieczeństwem pod kątem zgodności z aktualnymi założeniami bezpieczeństwa, obowiązującymi regulacjami prawnymi oraz dobrymi praktykami i standardami określonymi w:

- a) ustawie z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2026 r. poz. 20 ze zm.),
- b) § 20 ust. 2 Rozporządzenia 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).

W audycie zostanie uwzględniona analiza dokumentacji, obserwacje procesów, wywiady z personelem, testy techniczne – weryfikację konfiguracji systemów i testy podatności opisane w punkcie 4. Audyt zostanie przeprowadzony w siedzibie Zamawiającego oraz z wykorzystaniem dostępu zdalnego.

2. Dodatkowe kryteria prawne przy realizacji audytu

- a) Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. z 2018 r. poz. 1999),
- b) Rozporządzenie Ministra Cyfryzacji z dnia 10 września 2018 roku w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo (Dz.U. 2018 poz. 1780) - stosowane w zakresie niesprzecznym z nowelizacją z 2026 r.,

- c) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO),
- d) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 ze zm.).

3. Dokumentacja i raport z audytu

Wykonawca przekaze Zamawiającemu dokumentację z przeprowadzonego audytu zawierającą:

- a) plan audytu,
- b) opis przebiegu prac, testowanych systemów z wykonanymi testami i zastosowanymi do testów narzędziami,
- c) surowe wyniki skanów technicznych audytowanych systemów w postaci logów, zrzutów ekranów, udowadniające przeprowadzone testy aplikacji i infrastruktury sieciowej,
- d) listy kontrolne w postaci arkuszy pytań zadawanych audytowanym osobom,
- e) notatki z przeprowadzonych wywiadów z administratorem i personelem.

Wraz z dokumentacją przeprowadzonego audytu Wykonawca przekaze pisemny raport, zawierający:

- a) cel audytu, daty przeprowadzenia, skład zespołu audytorskiego, dane audytowanego podmiotu,
- b) opis w postaci nietechnicznej najważniejszych ryzyk i ogólnej oceny bezpieczeństwa
- c) opis zastosowanej metodyki audytu,
- d) opis zidentyfikowanych ryzyk oraz podatności wraz z oceną stopnia zagrożenia,
- e) wskazanie i omówienie niezgodności z wymaganiami prawnymi w odniesieniu do przepisów ustawy KSC oraz rozporządzenia KRI ze wskazaniem konkretnych artykułów,
- f) ocenę ryzyka rezydualnego,
- g) wnioski generalne,
- h) rekomendacje i zakres niezbędnych zmian organizacyjno-technicznych wraz z określonymi terminami realizacji,
- i) plan działań naprawczych,

Dokumentacja i raport z audytu zostaną przekazane Zamawiającemu w postaci elektronicznej jako osobne dokumenty podpisane kwalifikowanymi podpisami elektronicznymi audytorów.

4. Zakres przedmiotowy audytu

- a) identyfikacja systemów teleinformatycznych służących do świadczenia usług kluczowych oraz obowiązujących procedur,

b) weryfikacja procedur systemu zarządzania bezpieczeństwem informacji w zakresie ich kompletności, aktualności oraz praktycznego stosowania,

c) ocena zabezpieczeń technicznych:

- weryfikacja i analiza bezpieczeństwa dostępu do wewnętrznej infrastruktury sieciowej IT,
- weryfikacja i analiza jakościowa odporności infrastruktury IT na nieautoryzowane rozpoznanie jego składowych, w tym weryfikacja podatności serwisów DNS,
- weryfikacja systemów oraz protokołów zarządzania i monitorowania infrastruktury IT,
- weryfikacja jakościowa ochrony przed oprogramowaniem szkodliwym poprzez próby propagacji testowego oprogramowania szkodliwego. (zarówno z zewnątrz jak i od wewnątrz infrastruktury IT),
- weryfikacja środków technicznych kontroli dostępu do systemów operacyjnych, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania,
- weryfikacja i analiza danych przetwarzanych przez systemy logowania,
- weryfikacja podatności logicznych środków kontroli dostępu wewnątrz Infrastruktury IT,
- weryfikacja podatności systemów i sieci na ataki takie jak sniffing, spoofing, man-in-the-middle,
- weryfikacja na podstawie otwartości portów, podatności związanych z autoryzacją dostępu zdalnego do zasobów IT i ocena związanych z tym ryzyk,
- weryfikacja nieautoryzowanego dostępu do informacji o rodzaju i wersji wykorzystywanego oprogramowania systemowego i usługowego,
- weryfikacja arbitralnego i nieautoryzowanego zarządzania cyklem zmian systemów operacyjnych na urządzeniach infrastruktury IT,
- rozpoznanie i ocena mechanizmów zarządzania aktualizacjami - w tym obecność systemów automatyzujących propagację poprawek bezpieczeństwa,
- weryfikacja podatności na nieautoryzowane połączenia systemów VoIP,
- weryfikacja podatności hostów na ataki w warstwie systemowej (przy wykorzystaniu exploitów),
- weryfikacja podatności hostów na możliwość uzyskania nieautoryzowanego dostępu do zasobów plikowych,
- weryfikacja poufności przesyłu danych przetwarzanych na udostępnionych zasobach plikowych,

- weryfikacja podatności ustawień hostów na możliwość uzyskania nieautoryzowanego zdalnego dostępu do kontroli treści przesyłanych przez przeglądarki www,
- weryfikacja nieautoryzowanej dostępności do danych o czasie pracy, krytycznych systemów,
- weryfikacja obecności domyślnych kont użytkowników oraz haseł,
- weryfikacja bezpieczeństwa informacji zawartych w komunikatach systemów,
- weryfikacja obecności podatnych algorytmów szyfrowania,
- weryfikacja podatności systemów i aplikacji www w wewnętrznej infrastrukturze IT,
- weryfikacja poufności przesyłania danych do wydruku,
- analiza i ocena dodatkowych systemów bezpieczeństwa tj. dodatkowego oprogramowania antywirusowego, oprogramowania weryfikującego integralność systemów i gwarantującego audytowalność infrastruktury IT,
- weryfikacja podatności systemu sieci wewnętrznej na zakłócenie/zablokowanie dostępności do usług i określenie zasięgu oraz zlokalizowanie fizycznego źródła ataku,
- weryfikację reakcji oprogramowania AV poczty elektronicznej na rozsyłanie zagrożeń zawierających w treści zagrożenia, przesyłanych z wewnątrz i zewnątrz infrastruktury IT,
- badanie podatności systemu poczty na próby nieautoryzowanego dostępu do skrzynek poczty elektronicznej pracowników,
- badanie podatności systemu dostępu przez www do poczty elektronicznej,
- weryfikację bezpieczeństwa transmisji danych pomiędzy serwerem Active Directory a stacjami roboczymi,
- weryfikację reakcji i czasu reakcji na atak account lockout w domenie,
- weryfikację bezpieczeństwa poufności przesyłanych danych potrzebnych do autoryzacji, z urządzeń zintegrowanych z AD,
- weryfikację bezpieczeństwa poufności instrukcji GPO pod kątem ujawniania krytycznych informacji o systemach i wycieku danych.

d) Testy OSINT

- analiza informacji zawartych w nagłówkach odpowiedzi aplikacji www,
- analiza informacji zawartych w odpowiedziach aplikacji www,
- próba wykrycia luk i podatności konfiguracyjnych,
- analiza metadanych plików,

- próba enumeracji zasobów danych.

e) Testy aplikacyjne

- próba przeprowadzenia ataku słownikowego na hasła użytkowników,
- próba ujawnienia wycieków danych (obecność popularnych plików, analiza informacji o błędach, niewłaściwe nazewnictwo zasobów, wycieki kodu aplikacji),
- próby wywołania błędów aplikacji (manipulacja przesyłanymi danymi, w tym przesyłanie niepoprawnych danych, przesyłanie nadmiarowych danych, manipulacja parametrami oraz danymi nagłówkowymi zapytań,
- praktyczne sprawdzenie wykrytych podatności:
 - próba exploitacji z użyciem bazy posiadanych exploitów,
 - weryfikacja nieautoryzowanego dostępu do testowanego systemu,
 - weryfikacja informacji wrażliwych, uzyskanych w odpowiedziach systemu,
 - weryfikacja reakcji zabezpieczeń testowanego systemu, na przeprowadzane próby ataku.

f) Obsługa incydentów

- weryfikacja zdolności do wykrywania, rejestrowania, analizowania incydentów,
- wyznaczenie osoby (zespołu) odpowiedzialnej za utrzymanie kontaktów z podmiotami Krajowego Systemu Cyberbezpieczeństwa.

g) Zarządzanie ochroną danych osobowych (RODO)

Weryfikacja realizacji przez Zamawiającego czynności wymaganych przez Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016 / 679 z dnia 27 kwietnia 2016 r. obejmująca:

- weryfikacja realizacji przez Inspektora Ochrony Danych wymaganych czynności,
- weryfikacja czynności związanych z upoważnianiem do przetwarzania danych osobowych,
- weryfikacja poprawności powierzania przetwarzania danych osobowych, identyfikację procesów oraz systemów informatycznych służących do przetwarzania danych osobowych,
- rekomendacje związane z zapewnieniem skutecznego poziomu bezpieczeństwa ochrony danych osobowych.

h) Bezpieczeństwo fizyczne i środowiskowe

Weryfikacja skutecznej ochrony fizycznej i środowiskowej zasobów. obejmująca:

- weryfikacja granic obszaru bezpiecznego,
- weryfikacja zabezpieczeń wejścia/wyjścia,
- weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
- weryfikacja bezpieczeństwa okablowania strukturalnego,
- weryfikacja systemów chłodzenia,
- weryfikacja systemów alarmowych.

5. Przegląd i aktualizacja dokumentacji systemu zarządzania bezpieczeństwem informacji

Wykonawca zrealizuje następujące działania w zakresie dokumentacji bezpieczeństwa:

- a) optymalizacja posiadanych przez Zamawiającego dokumentów określających zasady zarządzania bezpieczeństwem informacji, o ile wyniki analizy ryzyka wykażą potrzebę takiej optymalizacji,
- b) weryfikacja i aktualizacja dokumentów określających zasady zarządzania bezpieczeństwem informacji, których brak stwierdzono po przeprowadzeniu analizy ryzyka.

6. Wymagane kwalifikacje po stronie Wykonawcy

- a) Wykonawca winien wykazać, że dysponuje lub będzie dysponować osobami spełniającymi wymagania określone w art. 15 ust. 1 ustawy o ksc (t.j. Dz.U. z 2026 r. poz. 20 ze zm.), w zakresie ilości audytorów (co najmniej dwóch) oraz posiadanych przez nich kwalifikacji - certyfikatów i praktyki.
- b) Audytorzy muszą posiadać przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999).
- c) Wykonawca złoży oświadczenie, że żaden z członków zespołu audytowego w ciągu 12 miesięcy poprzedzających rozpoczęcie audytu nie realizował na rzecz Zamawiającego zadań z zakresu:
 - wdrożenia lub utrzymania systemu zarządzania bezpieczeństwem informacji (SZBI),
 - obsługi incydentów bezpieczeństwa,
 - projektowania, wdrażania lub doradztwa w zakresie architektury bezpieczeństwa IT Zamawiającego.

7. Ankieta dojrzałości

Uwzględniając wyniki przeprowadzonego audytu Wykonawca wypełni końcową „Ankietę Dojrzałości Cyberbezpieczeństwa w Jednostkach Samorządu

Terytorialnego” opracowaną przez NASK-PIB, dostępną na stronie internetowej Konkursu „Cyberbezpieczny Samorząd” jako załącznik do regulaminu. Dane w ankiecie końcowej muszą być spójne z danymi z ankiety początkowej, udostępnionej przez Zamawiającego.

8. Zasoby zamawiającego uwzględnione w audycie

Zasoby i infrastruktura Zamawiającego obejmują:

- a) 1 główna lokalizacja z jedną serwerownią, dwie inne lokalizacje (USC i Straż Miejska z małą serwerownią) połączone w jedną sieć lokalną z lokalizacją główną,
- b) ok. 35 systemów serwerowych, większość Windows Serwer, ale też Linux i BSD, serwery działające w środowisku wirtualizacji Hyper-V (5 systemów hostowych dla maszyn wirtualnych, 3 macierze dyskowe), serwery DNS, www, poczty elektronicznej, EZD w ramach własnych zasobów,
- c) ok. 200 stacji roboczych/użytkowników Windows 10/11 (usługa Active Directory),
- d) 4 urządzenia NAS,
- e) ok. 50 przełączników sieciowych,
- f) sieć wi-fi odseparowana (vlan),
- g) sieć monitoringu odseparowana (vlan),
- h) 2 łącza internetowe i routery brzegowe w tym zaporą sprzętową,
- i) dokumentacja SZBI.