



## **OPIS PRZEDMIOTU ZAMÓWIENIA**

### **Zakres prac dla zadania:**

#### **„Audyt bezpieczeństwa oraz zgodność z Krajowymi Ramami Interoperacyjności”**

1. Głównym celem prac jest zapewnienie, że Zamawiający spełnia następujące wymagania:
  - 1.1. Wymagania wskazane w par. 15 Rozporządzenia Rady Ministrów „w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych” z dnia 12 kwietnia 2012 r. (zwane dalej Rozporządzeniem) w zakresie zarządzania bezpieczeństwem informacji i zarządzania usługami.
  - 1.2. Wymagania wskazane w par. 16-19 wspomnianego Rozporządzenia w zakresie funkcjonalności systemów informatycznych.
  - 1.3. Wymagania wskazane w par. 20-21 wspomnianego Rozporządzenia w zakresie zarządzania bezpieczeństwem informacji.
  - 1.4. Wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) (RODO).

### **Etap I.**

#### **Audyt bezpieczeństwa**

W skład audytu bezpieczeństwa wchodzić będą:

- I.1. Weryfikacja procedur bezpieczeństwa informacji, w tym dokumentacji w zakresie ochrony danych osobowych.**

## **I.2. Weryfikacja procedur szczegółowych w zakresie bezpieczeństwa IT.**

**Weryfikacja istniejących procedur (w formie spisanej lub funkcjonujących dobrych praktyk) związanych z technicznymi aspektami zabezpieczeń IT, takimi jak np.:**

- a) tworzenie i testowanie kopii zapasowych.
- b) raportowanie i zarządzanie incydentami bezpieczeństwa.
- c) zarządzanie kluczowymi systemami, w szczególności procedury aktualizacji komponentów programowych systemów i usług.
- d) sposób nadawania i weryfikowania uprawnień administratora systemu
- e) nadawanie i odbieranie uprawnień użytkowników systemów
- f) zdalny dostęp do sieci ZTM
- g) zabezpieczenie nośników danych
- h) zarządzanie i dokumentowanie zmian
- i) zasady przywracania systemów po przerwach w ich funkcjonowaniu

## **I.3. Test penetracyjny z zewnątrz z dedykowaną analizą usług kluczowych**

Podstawowym celem tej części prac jest stwierdzenie, na jakie niebezpieczeństwo narażona jest infrastruktura Zamawiającego (przy założeniu ataku z sieci Internet – a więc możliwego do przeprowadzenia przez dowolnego użytkownika sieci).

## **I.4. Test penetracyjny od wewnątrz**

Test penetracyjny od wewnątrz - social engineering, audyt ze stacji klienckiej, itp.

## **I.5. Szczegółowy raport z przeprowadzonych testów penetracyjnych**

Raport z Audytu będzie zawierał raport z przeprowadzonych testów penetracyjnych ze wskazaniem newralgicznych miejsc wraz z opisem sposobu ich naprawy.

## **I.6. Przegląd konfiguracji kluczowych systemów, usług i urządzeń:**

### **1. Systemy:**

- a) urządzenia sieciowe w liczbie 20.
- b) systemy zabezpieczeń (takie jak firewall, system antywirusowy, ewentualne inne rozwiązania jak system IDS/IPS lub narzędzia do weryfikacji integralności plików).

- c) systemy serwerowe w liczbie 11.
- d) reprezentatywna próba stacji roboczych (do 10 szt.), ze szczególnym uwzględnieniem stacji roboczych, na których są przetwarzane dane osobowe

## 2. Usługi:

- a) usługa Active Directory
- b) usługa poczty elektronicznej (jako uzupełnienie testów penetracyjnych ww. usługi)
- c) serwery Web (6 szt.) oraz środowiska uruchomieniowe aplikacji Web (6 szt.)
- d) serwery bazodanowe (3 szt.)
- e) systemy składowania danych (3 szt.) i serwery plików (2 szt.)
- f) kluczowe usługi sieciowe (jak DHCP, NTP)
- g) kluczowe aplikacje Web w sieci wewnętrznej (4 szt.)
- h) aplikacja do monitorowania sieci (2 szt.)
- i) środowisko wirtualizacji VMWare (4 szt.)

Oprócz wyżej wymienionych, w zależności od wyników penetracyjnego testu zewnętrznego lub wewnętrznego, powinny zostać zrealizowane dodatkowe dedykowane testy dla poszczególnych usług. Dla przykładu, w przypadku usługi poczty elektronicznej nastąpi weryfikacja specyficznych parametrów konfiguracyjnych serwera SMTP, np. pod kątem możliwości generowania niepożądanych raportów niedoręczenia (ang. unsocialized non-delivery report), wysyłania poczty z lokalnej domeny do zewnętrznych odbiorców, występowania mechanizmów automatycznych odpowiedzi, ustawień mechanizmów antyspamowych.

### **I.7. Raport z Audytu bezpieczeństwa informacji**

Wykonawca przygotowuje szczegółowy Raport z Audytu, zawierający następujące elementy:

1. Informację o spełnieniu wymagań wyszczególnionych w § 1 Umowy.
2. Raport dla Kierownictwa – zawierający, napisane językiem nietechnicznym, odpowiednim dla wyższej kadry kierowniczej – podsumowanie oceny infrastruktury z punktu widzenia bezpieczeństwa oraz ewentualne inne wnioski, będące wynikiem

przeprowadzonych testów. Raport ten zostanie zaprezentowany na spotkaniu z udziałem kierownictwa.

3. Szczegółowe rezultaty zrealizowanych testów wraz z podaniem odpowiednich metryk, opisem skojarzonych zagrożeń, a także sugestiami polepszenia bezpieczeństwa. Jeżeli będzie to możliwe, wskazane zostaną różne opcje postępowania z odmiennym stosunkiem kosztu do stopnia poprawy odporności na ataki.
4. W zakresie zauważonych w trakcie testów błędów bezpieczeństwa dowolnego rodzaju dla wszystkich spostrzeżonych luk zostaną zaraportowane:
  - Poziom krytyczności
  - Sposób wykrycia luki
  - Opis zagrożeń skojarzonych z luką
  - Rekomendacje Wykonawcy na poziomie pojedynczej luki wraz z instrukcją usunięcia luki

Ponadto, jeśli zespół audytorski zauważy, że wykazane luki bezpieczeństwa pozwalają wyciągnąć wnioski ogólne co do nieodpowiedniego poziomu bezpieczeństwa badanych systemów bądź usług, wnioski takie zostaną również wskazane w raporcie.

Raport będzie przygotowany w języku polskim. Dokument zostanie przekazany w formie elektronicznej oraz w formie papierowej (w 2 egzemplarzach). Ponadto o ewentualnych błędach wysoce krytycznych wykrytych podczas prac realizowanych z zewnątrz Zamawiający zostanie poinformowany niezwłocznie.

Raport z audytu zostanie przekazany Zamawiającemu w sposób opisany w § 4 Umowy.

## **Etap II.**

### **Szkolenia**

Wykonawca przygotuje oraz przeprowadzi w siedzibie Zamawiającego lub online, szkolenie z zakresu bezpieczeństwa informacji przeznaczone dla pracowników IT i innych wyznaczonych osób.

Tematyka szkolenia będzie dotyczyła zasad bezpieczeństwa teleinformatycznego z uwzględnieniem specyfiki funkcjonowania jednostki, w świetle wymagań KRI i normy ISO 27001. Czas trwania szkolenia: 2,5 godz. + 0,5 godz. na pytania/odpowiedzi; dwie grupy szkoleniowe. Szkolenie powinno zostać przeprowadzone w dwóch różnych dniach roboczych, w terminach i godzinach uzgodnionych z Zamawiającym.

Materiały przygotowane na szkolenie zostaną przekazane Zamawiającemu w formie pisemnej i elektronicznej. Każdy z uczestników szkolenia otrzyma imienny certyfikat ukończenia szkolenia ze wskazaniem zakresu, jakie ono obejmowało.

Szkolenia (Etap II) mogą zostać zrealizowane w trakcie trwania Etapu I.

### **Etap III**

#### **Omówienie wyników audytu**

Wykonawca przedstawi omówienie wyników audytu na spotkaniu z Kierownictwem ZTM. Spotkanie może zostać przeprowadzone w formie zdalnej lub stacjonarnie w siedzibie ZTM.

#### **Poufność informacji**

Informacje uzyskane w trakcie realizacji projektu są znane jedynie osobom zaangażowanym w jego realizację ze strony Wykonawcy oraz przekazywane wskazanym pracownikom Zamawiającego. Dodatkowo w trakcie prac może zająć konieczność wymiany informacji wrażliwych związanych ze zrealizowaną usługą. W takim wypadku ustala się:

1. Wykorzystanie do wymiany danych zabezpieczonych kryptograficznie mechanizmów poczty elektronicznej (GPG/PGP), przy użyciu co najmniej 2048-bitowych kluczy asymetrycznych,
2. Przesyłanie danych w archiwum ZIP, zaszyfrowanym przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczonym co najmniej 20-znakowym hasłem jednorazowym, przesłanym przez alternatywny kanał komunikacji (np. SMS).