

## 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 szczególności dokumentacji w zakresie ochrony danych osobowych.** Ocena, czy zachodzi konieczność przeprowadzenia oceny skutków przetwarzania dla ochrony danych (DPIA) oraz w przypadku zidentyfikowania takiej konieczności, dokonanie analizy DPIA.

#### **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.

#### **I.2. 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 napastnika).

#### **I.3. Test penetracyjny od wewnątrz**

Test penetracyjny z zewnątrz - social engineering, audyt ze stacji klienckiej, itp.

**I.4. Szczegółowy raport z przeprowadzonych testów penetracyjnych ze wskazaniem newralgicznych miejsc.****I.5. 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 mogą 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.6. Raport z audytu bezpieczeństwa**

Wykonawca przygotuje szczegółowy raport z prac, zawierający następujące elementy:

1. Streszczenie dla Kierownictwa – zawierający, napisane językiem nietechnicznym, odpowiednim dla wyższej kadry kierowniczej – podsumowanie oceny infrastruktury z punktu widzenia bezpieczeństwa oraz ewentualne inne wnioski natury ogólnej będące wynikiem przeprowadzonych testów.
2. Szczegółowe rezultaty zrealizowanych testów wraz z podaniem odpowiednich metryk, opisem skojarzonych zagrożeń, a także sugestiami polepszenia sytuacji. Jeżeli będzie to możliwe, wskazane zostaną różne opcje postępowania z odmiennym stosunkiem kosztu do stopnia poprawy odporności na ataki.
3. 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. Wykonawca zapewni iterację treści raportu z kadrą techniczną Zamawiającego przed przekazaniem ostatecznej wersji dokumentu. Celem takiej weryfikacji jest wykrycie ewentualnych nieścisłości wynikłych z faktu niedostatecznej znajomości specyfiki infrastruktury Zamawiającego przez zespół audytorski.

## **Etap II. Audyt zgodności z KRI oprogramowania finansowo-księgowego oraz kadrowego firmy Agrobex**

### **II.1. W szczególności następujące zagadnienia:**

- Weryfikacja systemu pod względem zasady poufności,
- Uwierzytelnienia w systemie,
- Identyfikacja,
- Konto użytkownika,
- Rozliczalność,
- Minimalne wymagania dla systemów teleinformatycznych

### **II.2. Raport z audytu oprogramowania finansowo-księgowego oraz kadrowego firmy Agrobex**

Wykonawca przygotuje szczegółowy raport z prac, zawierający następujące elementy:

4. Streszczenie dla Kierownictwa – zawierający, napisane językiem nietechnicznym, odpowiednim dla wyższej kadry kierowniczej – podsumowanie oceny badanego oprogramowania z punktu widzenia KRI oraz ewentualne inne wnioski natury ogólnej będące wynikiem przeprowadzonych testów.
5. Szczegółowe rezultaty zrealizowanych testów wraz z podaniem odpowiednich metryk, opisem skojarzonych zagrożeń, a także sugestiami polepszenia sytuacji. Jeżeli będzie to możliwe, wskazane zostaną różne opcje postępowania z odmiennym stosunkiem kosztu do stopnia poprawy obecnego stanu niezgodności z KRI.

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. Wykonawca zapewni iterację treści raportu z kadrą techniczną Zamawiającego przed przekazaniem ostatecznej wersji dokumentu. Celem takiej weryfikacji jest wykrycie ewentualnych nieścisłości wynikłych z faktu niedostatecznej znajomości specyfiki wskazanego w na tym Etapie oprogramowania Zamawiającego przez zespół audytorski.

**Etap III. Szkolenia**

Wykonawca przygotowuje oraz przeprowadzi w siedzibie Zamawiającego lub online całoniedniowe szkolenie z zakresu bezpieczeństwa informacji przeznaczone dla Kadry technicznej oraz dla pracowników. Szkolenie dla kadry technicznej zawierać będzie przeważającą ilość elementów warsztatowych.

Tematyka szkolenia będzie następująca: (czas trwania min. 6 h)

1. Omówienie wyników audytu bezpieczeństwa informacji w zakresie ochrony danych osobowych.
2. Omówienie wyników audytu bezpieczeństwa teleinformatycznego – sposoby ochrony przed wykrytymi zagrożeniami oraz metody unikania zauważonych odstępstw od zaleceń i dobrych praktyk bezpieczeństwa.
3. Przygotowanie Kadry Technicznej do realizacji corocznego audytu wewnętrznego w zakresie technicznego bezpieczeństwa informacji oraz odporności na ataki IT.
4. Przygotowanie Kadry Technicznej do realizacji corocznego audytu wewnętrznego w zakresie Systemu Zarządzania Bezpieczeństwem Informacji.
5. Zasady aktualizacji Systemu Zarządzania Bezpieczeństwem Informacji, przygotowanie Kadry technicznej do samodzielnego aktualizowania SZBI.

Materiały prezentacyjne przygotowane na szkolenie zostaną przekazane Zamawiającemu. Każdy z uczestników szkolenia otrzyma imienny certyfikat ukończenia szkolenia z wskazaniem zakresu materiału, jakie ono obejmowało.

**Poufność informacji**

Informacje uzyskane w trakcie realizacji projektu są znane jedynie osobom zaangażowanym w jego realizację ze strony Wykonawcy oraz przekazywane wskazanym pracownikom Zamawiającego. Jeżeli takie będzie życzenie Zamawiającego, poufność informacji zapewniona może zostać w sposób formalny w wyniku podpisania przez Strony umowy o nieujawnianiu danych. Dodatkowo w trakcie prac może zająć konieczność wymiany wrażliwych informacji związanych ze zrealizowaną usługą. W takim wypadku proponuje 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).