Załącznik nr 1 do zapytania ofertowego nr.....

Opis przedmiotu zamówienia

Przedmiotem zamówienia jest usługa:

Usługa przeprowadzenia audytu oraz diagnozy poziomu bezpieczeństwa teleinformatycznego (cyberbezpieczeństwa) i rekomendacji dotyczących podniesienia tego poziomu jako dwu etapowego audytu bezpieczeństwa systemu informacyjnego i ochrony danych medycznych zgodnie z „Wymaganiami dotyczącymi audytu bezpieczeństwa", stanowiącymi załącznik nr 2 do Umowy o finansowanie ze środków pochodzących z Funduszu Przeciwdziałania COVID-19 podniesienia poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców, będącej załącznikiem Nr 2 do Zarządzenia Nr 68/2022/BBIICD Prezesa NFZ z dnia 20 maja 2022 r. ,z wymaganiami ustawy z dnia 13 sierpnia 2018 roku o Krajowym Systemie Cyberbezpieczeństwa , Krajowych Ram Interoperacyjności zgodnie z wymaganiami norm PN ISO IEC 27001, PN ISO IEC 22301 wraz z wykorzystaniem standardów WGITA oraz NSC poprzez dwukrotne tożsame zadaniowo badanie:

a) spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,

b) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

c) określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

w zakresie:

- skuteczności działania infrastruktury,
- procesów zarządzania bezpieczeństwem informacji,
- monitorowania i reagowania na incydenty bezpieczeństwa,
- zarządzania ciągłością działania,
- utrzymania systemów informacyjnych,
- zarządzania bezpieczeństwem i ciągłością działania łańcucha usług

każdorazowe badanie:

- spełniania wymogów dokumentacyjnych obowiązujących u Zamawiającego jako regulacji wewnętrznych dokumentacji normatywnej i operacyjnej dotyczących usługi

kluczowej bezpieczeństwa informacji - dokumentacja SZBI/KRI/BCM , ochrony danych osobowych dokumentacja RODO i ODO ,

- określenia poziomu i dojrzałości bezpieczeństwa systemu informatycznego Zamawiającego w tym przeprowadzenia testów penetracyjnych

Zakres audytu

Ocena stopnia dojrzałości i zgodności organizacyjno - technicznej infrastruktury ICT w kontekście zabezpieczeń konfiguracji, eksploatacji projektu modernizacji ICT jako Operatora usługi Kluczowej , funkcjonującego u Zamawiającego jako realizację czynności:

Audyt organizacyjny polegający na:

a) weryfikacji środków organizacyjnych (w tym dokumentacja SZBI) w obszarze bezpieczeństwa informacji, w tym danych osobowych;

b) weryfikacji procesów i czynności przetwarzania danych uwzględniając ich charakter, zakres, kontekst, cele przetwarzania, zasoby, aktywa i ryzyka

c) weryfikacji realizowania przez pracowników obowiązków wynikających z regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI/BCM/ODO).

Wykaz obowiązków pracowników podlegających weryfikacji (poszczególnych procedur, instrukcji, zapisów z dokumentacji SZBI) zostanie przedłożony Wykonawcy po podpisaniu umowy. Weryfikacja musi obejmować przynajmniej kierownika lub zastępcę kierownika każdej komórki organizacyjnej oraz jej pracowników (chyba, że komórka posiada mniejszą liczbę pracowników - wówczas wszystkich jej pracowników).

Audyt bezpieczeństwa fizycznego

Badanie polega na polegający na weryfikacji środków technicznych służących zabezpieczeniu informacji, w tym danych osobowych, w szczególności stanu bezpieczeństwa fizycznego i środowiskowego siedziby Zamawiającego - budynki i pomieszczenia na podstawie wizji lokalnej obszarów przetwarzania danych.

Audyt teleinformatyczny

Badanie polega na wykonaniu czynności audytowych na wybranej reprezentatywnej próbie i przeprowadzeniu nieinwazyjnych (wewnętrznych i zewnętrznych) testów penetracyjnych systemów informatycznych w szczególności odniesieniu do infrastruktury sieciowej, systemu Firewall, aplikacji, portali i wybranych serwisów www oraz poczty elektronicznej jako:

SP ZOZ Zespół Szpitali Miejskich
w Chorzowie
ul. Strzelców Bytomskich 11
41-500 Chorzów
tel.: (32) 349 92 25
fax: (32) 241 39 52
zsm@zsm.com.pl
www.zsm.com.pl
NIP: 6271923530
REGON: 271503410
KRS: 0000011939

1. weryfikacji bezpieczeństwa infrastruktury sieciowej w szczególności:

   a) inwentaryzacja urządzeń sieciowych (adresy IP, konfiguracja urządzeń, konfiguracja zapory ogniowej, podział na sieci logiczne i fizyczne) w siedzibie Zamawiającego

   b) analiza urządzeń i ich parametrów technicznych zapewniających stronie Zamawiającej dostęp do sieci Internet - w tym serwera brzegowego, urządzeń UTM, Firewall, routerów;

   c) analiza konfiguracji sieci lokalnej;

   d) analiza oprogramowania wykorzystywanego przez Zamawiającego w zakresie zabezpieczenia informatycznego;

   e) analiza sposobu połączenia segmentów pomiędzy sobą;

   f) analiza metody komunikacji pomiędzy segmentami sieci.

   g) analiza zabezpieczenia ciągłości działania

2. weryfikacji bezpieczeństwa infrastruktury serwerowej w szczególności:

   a) analiza bezpieczeństwa zainstalowanych usług (czy zainstalowane oprogramowanie jest aktualne, czy zainstalowane oprogramowanie posiada znane luki w bezpieczeństwie, kto ma dostęp do udostępnionych usług);
   b) analiza bezpieczeństwa serwerów pod kątem dostępu użytkowników (czy jedynie uprawnieni użytkownicy mają dostęp do usług, czy udostępnione usługi zawierają jedynie te dane które są wymagane);
   c) analiza bezpieczeństwa uprawnień poszczególnych użytkowników oraz grup użytkowników;
   d) analiza bezpieczeństwa fizycznego infrastruktury serwerowej,
   e) analiza zabezpieczenia ciągłości działania

3. weryfikacji bezpieczeństwa poczty elektronicznej, domeny, stron internetowych Zamawiającego wg wymagań WCGA 2.1

4. weryfikacji bezpieczeństwa systemów (aplikacji) w których przetwarzane są dane osobowe:

   a) analiza podatności komponentów aplikacji, w tym serwerów aplikacyjnych i baz danych - próby uzyskania dostępu do panelu administracyjnego za pomocą kont zwykłych użytkowników m. in. przez wykorzystanie bieżącej sesji, podniesienie uprawnień, próby uzyskania większych uprawnień, próby uzyskania nieautoryzowanego dostępu do danych znajdujących się w systemie;

   b) analiza szyfrowania danych dla danych przesyłanych przez sieci publiczne.

   c) Wykaz systemów w których przetwarzane są dane w tym dane osobowe w weryfikacji bezpieczeństwa stacji roboczych:

SP ZOZ Zespół Szpitali Miejskich
w Chorzowie
ul. Strzelców Bytomskich 11
41-500 Chorzów
tel.: (32) 349 92 25
fax: (32) 241 39 52
zsm@zsm.com.pl
www.zsm.com.pl
NIP: 6271923530
REGON: 271503410
KRS: 0000011939

- analiza kontroli dostępu do stacji roboczych,

- analiza zainstalowanego oprogramowania znajdującego się na stacjach roboczych,

- analiza bezpieczeństwa stacji roboczych pod kątem zainstalowanych usług, dostępów zdalnych do stacji roboczych, bezpieczeństwa ochrony antywirusowej.

d) analiza zabezpieczenia ciągłości działania

5. weryfikacji zarządzania kopiami zapasowymi i ciągłością działania w szczególności:

a) analizę poprawności wykonywanych kopii zapasowych,

b) analiza częstotliwości wykonywania kopii zapasowych,

c) analiza bezpieczeństwa wykonywanych kopii zapasowych,

d) analiza testów odzyskiwania kopii zapasowych - odtwarzania danych w środowisku testowym,

e) analiza zbierania, przechowywania i monitorowania logów systemowych,

6. weryfikacji poprawności realizacji w zakresie:

a) zarządzania hasłami użytkowników i hasłami administracyjnymi,

b) instalacji i aktualizacji oprogramowania,

c) ochrony przed szkodliwym oprogramowaniem,

d) zabezpieczania procesu pracy zdalnej,

e) rozwoju systemów informatycznych,

f) zarządzania zmianami w systemach informatycznych,

g) przeglądów, konserwacji i napraw systemu informatycznego,

h) monitorowania bezpieczeństwa systemów informatycznych

i) zapisywanie, monitorowanie, zabezpieczanie logów systemowych,

j) monitorowania pojemności i wydajności systemów informatycznych,

k) bezpieczeństwa sieci,

l) zapewnienia legalności oprogramowania,

m) usuwania danych i niszczenia nośników,

n) synchronizacji zegarów

o) gromadzenia logów

•• SP ZOZ Zespół Szpitali Miejskich
w Chorzowie
ul. Strzelców Bytomskich 11
41-500 Chorzów

•• tel.: (32) 349 92 25
fax: (32) 241 39 52

•• zsm@zsm.com.pl
www.zsm.com.pl

•• NIP: 6271923530
REGON: 271503410
KRS: 0000011939

W czasie wykonania i po wykonaniu usługi infrastruktura Zamawiającego musi pozostać w niezmienionej formie, tj. nie może zostać uszkodzona, jak również nie mogą zostać usunięte, zmienione, nadpisane dane znajdujące się w tej infrastrukturze. Zamawiający dopuszcza wykonanie audytu w formie hybrydowej.

Raport

Wynikiem przeprowadzonych obu etapów audytów i testów będzie raport po-audytowy w standardzie ENISA zawierający:

1. przedmiot, cel i zakres audytu,
2. datę rozpoczęcia audytu,
3. opis przyjętej metodyki,
4. raport dla kierownictwa obejmujące syntezę wyników audytu i ocenę poziomu spełnienia wymogów RODO, KRI, regulacji wewnętrznych dot. bezpieczeństwa informacji Zamawiającego oraz ocenę bezpieczeństwa systemu informatycznego w tym podsumowanie zidentyfikowanych słabości/nieprawidłowości, a także główne rekomendacje dotyczące poprawy bezpieczeństwa informacji, danych i systemu informatycznego.
5. dokładny opis zidentyfikowanych nieprawidłowości w szczególności
   - wskazujący miejsca, w których występują realne bądź potencjalne problemy z bezpieczeństwem informacji;
   - zawierający wyniki audytów, w tym testów i ich interpretację - ustalenia musza odnosić się do konkretnych przypadków słabości/nieprawidłowości popartych zgromadzonymi dowodami audytowymi, które będą stanowiły załącznik do raportu;
   - zawierający rekomendacje w zakresie eliminacji zidentyfikowanych słabości/nieprawidłowości oraz poprawy poziomu bezpieczeństwa, w tym wskazanie działań korygujących i/lub doskonalących bez lokowania sprzętu lub oprogramowania.
6. analizę rekomendowanych zmian w treści regulacji wewnętrznych dot. bezpieczeństwa informacji, w tym danych osobowych (dokumentacja SZBI) Zamawiającego wraz z proponowaną treścią nowych (zmienionych lub dodanych) zapisów;
7. wypełniony Formularz weryfikacji dojrzałości organizacji pod kątem cyberbezpieczeństwa
8. datę sporządzenia raportu;
9. imiona i nazwiska audytorów realizujących zadanie oraz ich podpisy.

W terminie do 21 dni od daty zakończenia audytu w siedzibie Zamawiającego Wykonawca prześle w formie elektronicznej w formacie edytowalnym i pdf raport, zaszyfrowany programem 7 ZIP przy użyciu algorytmu szyfrującego AES-256 oraz zabezpieczony co najmniej 11-znakowym hasłem jednorazowym przesłanym przez alternatywny kanał komunikacji.

Wykonawca może dodatkowo przekazać raport końcowy w wersji edytowalnej w formacie A4 .

Zakres czasowy audytu

1. Czynności audytowe w siedzibie Zamawiającego powinny zakończyć się w ciągu do 21 dni kalendarzowych od daty rozpoczęcia audytu w siedzibie Zamawiającego.

Podstawowe informacje na temat systemów informatycznych Zamawiającego

liczba komputerów:

stacjonarnych – 650

przenośnych – 21

liczba serwerów:

fizycznych - 23

wirtualnych - 28

liczba serwerów:

Windows - 39

Linux - 12

liczba aplikacji bazodanowych - *systemów przetwarzających dane i dane osobowe - 19*

liczba serwerowni - 2

liczba urządzeń sieciowych - (drukarki, routery , switche, voip, itd.) – 300

liczba Access Point - 57

liczba drukarek sieciowych - 101

liczba podsieci - 4

liczba adresów zewnętrznych – 9

wdrożony Active Directory - tak

liczba serwisów www - 6

P.O.
Dyrektora operacyjnego
SP ZOZ Zespół Szpitali Miejskich

Iwona Filip