SAMODZIELNY PUBLICZNY
ZESPÓŁ OPIEKI ZDROWOTNEJ
22-300 Krasnystaw
ul. Sobieskiego 4
tel. 82 543 15 22, fax 82 576 49 01
NIP 564-14-75-805

FP-Z.19.2022

Krasnystaw 2022-08-08

Wykonawcy biorący udział w postępowaniu o udzielenie zamówienia o wartości szacunkowej netto nie przekraczającej 130 000 zł na

- usługę bezpieczeństwa systemów teleinformatycznych świadczeniodawców SP ZOZ w Krasnymstawie

Zamawiający informuje, że do w/w postępowania wpłynęły zapytania na które udziela odpowiedzi:

Pytanie 1 Szkolenia : ile grup oraz osób ma być przeszkolonych?
Odpowiedź: Szkolenie dla kadry Zarządzającej ok. 20 osób, oraz pozostałych pracowników 200-400 osób.

Pytanie 2 Pentesty: Czy możemy poprosić o opis środowiska którego mają dotyczyć testy penetracyjne ?
Odpowiedź: Testy penetracyjne zakończone raportem – Router dostawcy internetowego – urządzenie brzegowe UTM – przełączniki sieciowe (ok.30) – Macierz, serwery, stacje robocze (ok.200).

Pytanie 3 Czy audyty mają być przeprowadzone osobiście czy mogą być zdalnie?
Odpowiedź: Minimum jeden audyt przeprowadzony stacjonarnie. Posiadanie niezbędnych kwalifikacji do wykonania audytu, tj. oświadczenie do przeprowadzenia audytu zgodnie z wymogami zawartymi w załączniku nr 2 do umowy (Zarządzeniem NR 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022r.) wraz z wykazaniem certyfikatów uprawniających do przeprowadzenia audytu.
Ponadto Audyt końcowy potwierdzający zwiększenie poziomu Cyberbezpieczeństwa powinien być zakończony raportem w języku polskim, przekazany zamawiającemu w formie papierowej oraz elektronicznej.

Pytanie 4 Jaka będzie liczba uczestników szkolenia?
Odpowiedź: Szkolenie dla kadry zarządzającej ok. 20 osób, oraz pozostałych pracowników 200 do 400 osób.

Pytanie 5 Ile godzin szkoleniowych chcielibyście Państwo przeznaczyć dla każdego z uczestników?
Odpowiedź: max 1 – 1,5h

Pytanie 6 Jak duże grupy szkoleniowe państwo przewidujecie?
Odpowiedź: Nie mamy żadnych preferencji, mogą być grupy 20 – 40 osobowe.

Pytanie 7 Szkolenie ma zostać zrealizowane w formie zdalnej czy stacjonarnej?
Odpowiedź: Wymagamy szkolenia zdalnego (online), dopuszczamy szkolenie stacjonarne

Pytanie 8 Czy w przypadku szkolenia stacjonarnego jednostka udostępnia odpowiednie miejsce
Odpowiedź: Tak, Zamawiający udostępni odpowiednie miejsce.

Pytanie 9 Czy oczekujecie Państwo przygotowania materiałów dydaktycznych w formie papierowej dla każdego z uczestników szkolenia?
Odpowiedź: Zamawiający oczekuje materiałów w formie elektronicznej

Pytanie 10 Czy oczekujcie Państwo wręczenia każdemu z uczestników zaświadczenia/certyfikatu odbycia szkolenia?
Odpowiedź: Wymagamy listy imiennej zaświadczającej o odbyciu szkolenia przez pracowników, dopuszczamy możliwość wystawienia imiennych certyfikatów lub zaświadczeń dla pracowników

Pytanie 11 W zakresie przedmiotu zamówienia znajduje się zadanie „Opracowanie planu projektu, a także pomoc w przygotowaniu wymaganych dokumentów projektu.". Proszę o sprecyzowanie zakresu pomocy świadczonej Zamawiającemu oraz informację odnośnie zakresu projektu. Jakich zadań dotyczy wspomniana pomoc? Na czym polega projekt?
Odpowiedź: Ewentualna pomoc w opracowaniu dokumentów, które będą wymagane, aby spełnić warunki przyznawania i rozliczania środków na finansowanie działań w celu podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców.

Pytanie 12 Czy szkolenie z zakresu cyberbezpieczeństwa dla pozostałych pracowników szpitala może zostać przeprowadzone zdalnie (on-line), zamiast w formie systemu e-learningowego?
Odpowiedź: **TAK** może zostać przeprowadzone zdalnie (on-line).

Pytanie 13 Jaka jest przewidywana liczba uczestników szkoleń?
Odpowiedź: Szkolenie dla kadry Zarządzającej ok. 20 osób, oraz pozostałych pracowników 200-400 osób.

Pytanie 14 W zakresie zadań do zrealizowania jest zadanie „Audyt początkowy określający stopień spełnienia wymagań bezpieczeństwa informacji w zakresie normy CIS Controls przez Zamawiającego, oraz uwzględniający zasadność zakupu zaplanowanego sprzętu." Jaki sprzęt ma zostać zakupiony?
Odpowiedź: 2 x serwer pod backup, 1 x macierz, 1 x urządzenie UTM, oprogramowanie wirtualizacyjne (maszyny oraz backup).

Pytanie 15 Jakiej wielkości jest sieć podlegająca testom (szacowana liczba adresów IP i aktywnych hostów)?
Odpowiedź: Około 450 adresów z czego około 400 aktywnych hostów

Pytanie 16 Czy wszystkie prace mogą zostać zrealizowane zdalnie?
Odpowiedź: Zamawiający nie wyraża zgody na realizację wszystkich prac zdalnie.

Pytanie 17 Czy Zamawiający określa agendę szkoleń, czy też jest to po stronie Wykonawcy?
Odpowiedź: Agendę szkoleń ustala Wykonawca.

Pytanie 18 Czy Zamawiający wymaga posiadania przez Wykonawcę akredytacji zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 5)?
Odpowiedź:
Wykonawca musi mieć akredytacje LUB dysponować audytorami o odpowiednim doświadczeniu i certyfikacie.
W wymaganiach dotyczących audytu bezpieczeństwa określonych w Załączniku nr 2 do Umowy z Zarządzenia NR 68/2022/BBIICD PREZESA NARODOWEGO FUNDUSZU ZDROWIA punkty 1 i 2 należy traktować rozłącznie. Podmiot audytujący musi posiadać akredytację lub dysponować minimum dwoma audytorami spełniającymi dowolny z warunków a, b lub c.

Pytanie 19 Przełączniki sieciowe - czy testy mają objąć badanie konfiguracji urządzenia czy też nie ?
Odpowiedź: Tak, mają objąć badanie konfiguracji urządzenia.

Pytanie 20 Czy za serwerami kryją się aplikacje WEB które będą chcieli Państwo przetestować ? Jeżeli tak to bardzo proszę o podanie ich ilości.
Odpowiedź: Jedna aplikacja WEB – wyniki laboratoryjne on-linie.

Pytanie 21 w zapytaniu jest mowa o testach penetracyjnych, proszę o informację w jakim zakresie mają one być przeprowadzone (podstawowe skanowanie, exploitacja?)
Proszę o podanie informacji niezbędnych do wyceny testów:
- siedziby
- liczba komputerów
- liczba serwerów wirtualnych
- liczba serwerów fizycznych:
- łącza internetowe
- liczba urządzeń klasy UTM
- liczba urządzeń klasy Web Aplication Firewall
- serwery poczty e-mail
- liczba serwerowni
- liczba pomieszczeń teletechnicznych
- liczba szaf teletechnicznych

Odpowiedź: Wymagamy przeprowadzenie pełnych testów penetracyjnych. Podsumowaniem działań ma być raport w którym szczegółowo opisane będą wszystkie zidentyfikowane podatności oraz sposób ich usunięcia.
Pozostałe informacje:
- siedziby - 3 budynki
- liczba komputerów – około 200
- liczba serwerów wirtualnych – ok. 18
- liczba serwerów fizycznych – ok. 10
- łącza internetowe – 2
- liczba urządzeń klasy UTM – 1
- liczba urządzeń klasy Web Aplication Firewall – 0
- serwery poczty e-mail – 1
- liczba serwerowni – 2
- liczba pomieszczeń teletechnicznych – 2
- liczba szaf teletechnicznych – ok. 7

Pytanie 22 Proszę o wyszczególnienie dokumentacji, o której mowa w zapytaniu ofertowym.
Odpowiedź: Dokumenty, które będą wymagane, aby spełnić warunki przyznawania i rozliczania środków na finansowanie działań w celu

podniesienia poziomu bezpieczeństwa systemów teleinformatycznych u świadczeniodawców.

Pytanie 23 Proszę o podanie liczby uczestników szkolenia, informacji o liczbie szkoleń oraz informacji czy szkolenia mają być przeprowadzone stacjonarnie czy online
Odpowiedź: Szkolenie dla kadry Zarządzającej ok. 20 osób, oraz pozostałych pracowników 200-400 osób.

Pytanie 24 Piszę do Państwa z wyjaśnieniem treści zapytania ofertowego odnośnie przeprowadzenia audytu cyberbezpieczeństwa wraz ze szkoleniem. Ile jest osób do przeszkolenia i czy można ofertę złożyć przez pocztę elektroniczną?
Odpowiedź: Szkolenie dla kadry Zarządzającej ok. 20 osób, oraz pozostałych pracowników 200-400 osób. Zamawiający wyraża zgodę na złożenie oferty pocztą elektroniczną, na adres: sekretariat@spzozkrasnystaw.pl

Pytanie 25 prosze o przybliżone zwymiarowanie środowiska, które ma zostać poddane audytowi: ilość serwerow i stacji roboczych, urządzeń sieciowych, ilość sieci/podsieci, systemy segmentacji sieci (VLAN, VxLAN, NSX, itp), sieci bezprzewodowe (ile), systemy wirtualizacyjne (jakie, ile), systemy operacyjne (jakie, ile), koncentratory VPN (ile, jakie), systemy IDM (ile, jakie), systemy SIEM, itp.
Odpowiedź: ok.10 serwerów fizycznych w tym ok. 18 serwerów wirtualnych, macierz, ok. 200 stacji roboczych i ok. 30 przełączników połączonych w jednej podsieci; jedna sieć bezprzewodowa; system wirtualizacyjny VMWare; systemy operacyjne: Windows Server 2012 R2, Windows Server 2008 R2, Windows 10, Windows 7, Debian, RedHat, Ubuntu, CentOS; ok. 4 koncentratory VPN.

Pytanie 26 zgodnie z zapisami projektu umowy: "Wykonawca zrealizuje: Audyt początkowy określający stopień spełnienia wymagań bezpieczeństwa informacji w zakresie normy CIS Controls przez Zamawiającego, oraz uwzględniający zasadność zakupu zaplanowanego sprzętu." - audyt będzie stwierdzeniem stanu faktycznego, w jaki więc sposób ma on w rozumieniu Zamawiającego uwzględnić zasadność zakupu zaplanowanego sprzętu? Czy chodzi o szczegółowe rekomendacje wskazujące na potrzeby zakupowe? Czy "zaplanowany sprzęt" został określony?
Odpowiedź: Wykrycie nieprawidłowości oraz podatności stwierdzi podniesienie bezpieczeństwa poprzez zakup zaplanowanego sprzętu.

Pytanie 27 czy Zamawiający pisząc w zapytaniu o "testach penetracyjnych" ma na myśli faktyczne testy penetracyjne czy skanowania podatności (koszt wykonania testów penetracyjnych może być o rząd wielkości większy niż wykonania skanowań podatności, skanowania podatności są wykonywane automatycznie - testy penetracyjne muszą być wykonane przez doświadczonego pentestera lub zespół pentesterów, proszę też pamiętać że raport ze skanowań podatności nigdy nie będzie testem penetracyjnym, nawet jeśli skaner aktywnie próbuje wykorzystać znalezione podatności, otwarte dostępy lub domyślne hasła do systemów informatycznych)?

Odpowiedź: Wymagamy przeprowadzenie pełnych testów penetracyjnych. Podsumowaniem działań ma być raport w którym szczegółowo opisane będą wszystkie zidentyfikowane podatności oraz sposób ich usunięcia. Raport powinien składać się z następujących części:

- Cel i zakres
- Podejście, metodyka i narzędzia
- Metodyka szacowania ryzyka
- Streszczenie dla Kierownictwa
- Zidentyfikowane podatności i rekomendacje ich naprawy
- Dowody potwierdzające występowanie podatności
- Klasyfikację zidentyfikowanych podatności według CVSS

Pytanie 28 testy penetracyjne - jaka metodyka testów ma być zastosowana, jaki rodzaj testów penetracyjnych ma być zastosowany (blackbox, greybox, whitebox), jakie systemy mają być objęte testami penetracyjnymi, czy sa jakieś webaplikacje (jakie, ile), strony internetowe (jakie, ile), API (jakie, ile), sieci bezprzewodowe (ile), czy kontrola segmentacji sieci również ma być objęta zakresem pentestów?

Odpowiedź: Wymagamy przeprowadzenie pełnych testów penetracyjnych, zastosowana metodyka: NIST. Testy mają objąć całą infrastrukturę zewnętrzną i wewnętrzną szpitala, stronę wewnętrzna oraz jedną sieć bezprzewodową. Po usunięciu podatności wykonawca przystąpi do retestu. Podsumowaniem działań ma być raport w którym szczegółowo opisane będą wszystkie zidentyfikowane podatności oraz sposób ich usunięcia.

Pytanie 29 testy penetracyjne - retest ma dotyczyć jedynie wykrytych wcześniej (podczas pierwszego testu penetracyjnego) podatności czy ma być wykonany od nowa (ponownie cały zakres)?

- czy możliwe jest wykonanie testów penetracyjnych w formie zdalnej (np. z wykorzystaniem tunelu VPN)?

Odpowiedź: Testy penetracyjne mają objąć infrastrukturę zewnętrzną i wewnętrzną szpitala. Po usunięciu podatności wykonawca przystąpi do retestu. Wymagane jest przeprowadzenie testów w formie stacjonarnej.

Pytanie 30 zgodnie z zapisami projektu umowy szkolenia dla pozostałej części pracowników "mogą być dostarczone w formie dowolnego systemu e-learningowego wykorzystywanego przez Zamawiającego" - jakie systemy e-learningowe Zamawiający ma na myśli i czy można skorzystać z innego niż Zamawiającego systemu e-learningowego i hostowanego w infrastrukturze wykonawcy?
Odpowiedź: Szkolenie online dla wszystkich pracowników Zamawiającego. Wykonawca zapewni min. 3 terminy szkolenia w formie online. Każdy z pracowników powinien otrzymać indywidualne zaproszenie na szkolenie w formie maila. Platforma powinna umożliwić identyfikację pracownika. Po zakończonym szkoleniu wykonawca udostępni zamawiającemu szczegółowe informacje o liście obecności pracowników zamawiającego. Istnieje możliwość przeprowadzenia szkolenia w siedzibie Wykonawcy.

Pytanie 31 akcja Phishing - jaki zakres pracowników ma być poddany akcji? czy Zamawiający ma jakieś szczegółowe wymagania co do zakresu, sposobu czy raportu z wykonanej akcji?
Odpowiedź: Testy socjotechniczne (phishing), powinny objąć swoim działaniem wszystkich pracowników zamawiającego. Zamawiający udostępni pełną listę adresów e-mail. Szczegóły akcji powinny być ustalone i potwierdzone przez zamawiającego. Wynikiem testów ma być szczegółowy raport z przeprowadzonych działań.

Pytanie 32 w projekcie umowy widnieje Pan Grzegorz Surdyka tel. 516 016 406, e-mail: grzegorz.surdyka@sisoft.pl jako osoba kontaktowa - czy wskazana osoba jest przedstawicielem firmy trzeciej, która również uczestniczy lub będzie uczestniczyła w projekcie?
Odpowiedź: Wskazana osoba omyłkowa została wstawiona jako osoba kontaktowa, Zamawiający wnosi poprawkę w projekcie umowy.

Pytanie 33 audyt zgodnie CIS Controls ma być wykonany w wersji 7.1 czy 8?
Odpowiedź: Audyt może być wykonany w wersji 7.1 lub 8.

Pytanie 34 Dzień Dobry, mam pytanie odnośnie punktu e) w rozdziale XI zapytania dotyczące wymaganych dokumentów, a dokładnie zapisu o projekcie umowy załącznik nr 3. Czy umowa ma być wydrukowana oraz dołączona do

reszty dokumentów? czy dokument ma zostać zaparafowany i dołączony do reszty załączników?

Odpowiedź: Umowa ma być wydrukowana oraz dołączona do reszty dokumentów, natomiast dokument ma być zaparafowany.

Pytanie 35 Co do szkolenia zdalnego przy tak dużej ilości osób musimy podzielić na kilka grup. Pytanie czy z podziałem co do ilości grup macie Państwo jakieś preferencje?

Odpowiedź:

Nie mamy żadnych preferencji. (Mogą być grupy 20 – 40 osobowe).

DYREKTOR
Samodzielnego Publicznego Zespołu Opieki Zdrowotnej
w Krasnymstawie
Andrzej Jarzębowski

KIEROWNIK
Działu Informatyki
mgr Bartłomiej Wrona