OPIS PRZEDMIOTU ZAMÓWIENIA

1. Oznaczenia kodu CPV – Wspólnego Słownika Zamówień (kod i opis):
2. Główny kod CPV:
   79212000-3 - Usługi audytu
3. Dodatkowe kody CPV*:

…..-…..-…..-…..-….. ……
…..-…..-…..-…..-….. ……

2. Przedmiotem jest

Usługa audytu informatycznego w ramach działań Zamawiającego mających na celu podniesienie poziomu bezpieczeństwa systemów teleinformatycznych świadczeniodawców będącymi podmiotami leczniczymi

1. Celem audytu jest wykazanie przez świadczeniodawcę podniesienia poziomu bezpieczeństwa teleinformatycznego po zrealizowaniu czynności, zgodnie z zarządzeniem Nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia oraz w odniesieniu do stanu na dzień przeprowadzenia badania poziomu dojrzałości cyberbezpieczeństwa u świadczeniodawcy w formie ankiety. Przeprowadzony audyt wykaże podniesienie poziomu bezpieczeństwa teleinformatycznego w odniesieniu do poziomu wynikającego z ankiety lub jego brak. Raport musi zawierać jasne stanowisko audytora w zakresie wskazania, że spożytkowane środki wpłynęły na podniesienie poziomu bezpieczeństwa.
2. Zakres prac audytora będzie obejmować:
    1. Audyt Końcowy
        a. Usługa audytu końcowego zrealizowana zgodnie z wymogami Zarządzenia Prezesa Narodowego Funduszu Zdrowia z dnia 20 maja 2022 r.
        b. Zaktualizowana inwentaryzacja infrastruktury sieciowej (zewnętrzna I wewnętrzna).
        c. Zautomatyzowane i manualne wykrywanie potencjalnych podatności w zabezpieczeniach sieci i aplikacji internetowych.
        d. Pomiar poprawy stanu cyberbezpieczeństwa w porównaniu do audytu wstępnego.
        e. Szczegółowy raport wraz z rekomendacjami najlepszych praktyk.
3. Opis czynności
    1. Analiza obecnego stanu cyberbezpieczeństwa, punktów styku, systemów teleinformatycznych, środo-wisk aplikacyjnych, konfiguracji i segmentacji zasobów sieciowych.
    2. Prace audytowe wykonywane będą w 6 obszarach zgodnie z opisem **Obszary oraz opis działań skutkujących podniesieniu poziomu bezpieczeństwa teleinformatycznego**
    3. Wykonawca jest zobowiązany do:
        a. Bieżącego doradztwa na etapie tworzenia szczegółowego planu wdrożenia,
        b. Prowadzenia dokumentacji w języku Polskim
        c. Przygotowania wytycznych w zakresie zabezpieczenia w oparciu o normy i „najlepsze praktyki” stosowane w obszarze cyberbezpieczeństwa oraz obszarów wyznaczonych przez Prezesa Narodowego funduszu zdrowia

d. Przeprowadzenia audytu wstępnego w zakresie bezpieczeństwa informacji dla każdego z obszarów sprawdzanie oraz wskazanie zagrożeń i podatności oraz ocena aktualnego poziomu bezpieczeństwa
e. Przygotowania strategii modelowania zagrożeń:
   - Zbudowanie wzorca modelowania zagrożeń
   - Stworzenie strategii poprawy bezpieczeństwa na podstawie wymodelowanego wzorca uwzględniając rozwiązania hardware i software.
f. Przygotowanie szczegółowego planu przeprowadzenia audytu końcowego.
g. Przeprowadzenie audytu końcowego, którego celem będzie dostarczenie informacji o rzeczywistym podniesieniu poziomu bezpieczeństwa informacji oraz zastosowanych zabezpieczeniach, a także zgodności tego poziomu z wymaganiami określonymi w zarządzeniu Nr 68/2022/BBIICD Prezesa Narodowego Funduszu Zdrowia
h. Przeprowadzone audyty bezpieczeństwa dla każdego z obszarów będą sporządzone na protokole/raporcie z Audytu.

4. Przeprowadzone badania i analizy w trakcie audytu powinny wskazać zagrożenia i ryzyka wynikające z:
   a. Zastosowaniem technologii i standardów zabezpieczeń
   b. Słabości oprogramowania oraz poprawności konfiguracji komponentów takich jak:
      - Infrastruktura
      - Systemy sieciowe i serwerowe
      - Systemy bazodanowe
   c. Przeprowadzenia audytu procedur wykonywania i odtwarzania kopii zapasowych i backup-ów
   d. Audytu procedur na wypadek awarii
   e. Przeglądu architektury sieci pod kątem bezpieczeństwa teleinformatycznego jednostki

4. Efektem przeprowadzonych audytów będą:
   1. Dokument zawierający wytyczne z zakresu zabezpieczenia w oparciu o normy oraz „najlepszych praktyk" stosowanych w obszarze bezpieczeństwa systemów teleinformatycznych
   2. Raporty zawierające wnioski, zalecenia i rekomendacje mające na celu dokładne rozpoznanie i redukcję zidentyfikowanych zagrożeń, ryzyka, podatności oraz odstępstw od norm i dobrych praktyk wraz ze wskazaniem konkretnych działań naprawczych
   3. Raporty będą zawierały również:
      a. Obserwacje audytowe,
      b. Wyniki testów i ich interpretację,
      c. Listę wykrytych podatności opatrzonych komentarzem audytora wraz z ich kwalifikacją w zależności od stopnia ich znaczenia dla bezpieczeństwa,
      d. Wnioski z audytu
      e. Zalecenia i rekomendacje,
   4. Wykonawca zobowiązany jest do udziału w spotkaniach, które mogą zostać zorganizowane przez Zamawiającego w celu omówienia przygotowanych dokumentów, postępu prac i wyników prac audytowych

Obszary oraz opis działań skutkujących podniesieniu poziomu bezpieczeństwa teleinformatycznego

1. **Skuteczność działania infrastruktury**
    a. Urządzenia i konfiguracja w zakresie ochrony poczty
    b. Urządzenia i konfiguracja w zakresie ochrony sieci
    c. Urządzenia i konfiguracja w zakresie systemów serwerowych
    d. Urządzenia i konfiguracja w zakresie stacji roboczych
    e. Urządzenia i konfiguracja w zakresie systemów bezpieczeństwa
2. **Procesy zarządzania bezpieczeństwem informacji**
    a. Nośniki wymienne - udokumentowany sposób postępowania
    b. Zarządzanie tożsamością / dostęp do systemów w zakresie:
        i. Przydzielanie dostępu
        ii. Odbieranie dostępu
    c. Pomieszczenie w dyspozycji struktur zespołu odpowiedzialnego za cyberbezpieczeństwo w przypadku podmiotów, które otrzymały decyzję uznającą taki podmiot za operatora usługi kluczowej, o którym mowa w art. 5 ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa
3. **Monitorowanie i reagowanie na incydenty bezpieczeństwa**
    a. Procedury zarządzania incydentami
    b. Raportowanie poziomów pokrycia scenariuszami znanych incydentów
    c. Dokumentacja dotycząca przekazywania informacji do właściwego zespołu CSIRT poziomu krajowego / sektorowego zespołu cyberbezpieczeństwa
    d. Monitorowanie i wykrycie incydentów bezpieczeństwa
    e. Identyfikacja i dokumentowanie przyczyn wystąpienia incydentów
4. **Zarządzanie ciągłością działania**
    a. Konfiguracja oraz polityki systemów do wykonywania kopii bezpieczeństwa
    b. Raport z przeglądów i testów odtwarzania kopii bezpieczeństwa
    c. Procedury wykonywania i przechowywania kopii zapasowych
    d. Strategia i polityka ciągłości działania, awaryjne oraz odtwarzania po katastrofie (DRP)
    e. Procedury utrzymaniowe
5. **Utrzymanie systemów informacyjnych**
    a. Harmonogramy skanowania podatności
    b. Aktualny status realizacji postępowania z podatnościami
    c. Procedury związane ze z identyfikowaniem (wykryciem) podatności
    d. Współpraca z osobami odpowiedzialnymi za procesy zarządzania incydentami
6. **Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług**
    a. Polityka bezpieczeństwa w relacjach z dostawcami
    b. Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa
    c. Dostęp zdalny
    d. Metody uwierzytelnienia

Informacje Techniczne

1. Celem przeprowadzenia testów bezpieczeństwa jest podniesienie poziomu bezpieczeństwa jednostki
2. Web Aplikacja służy do obsługi medycznej szpitala – prowadzenia dokumentacji medycznej
3. Wszystkie systemy Zamawiającego są wrażliwe/krytyczne i wymagają zachowania szczególnej ostrożności przy ich testowaniu
4. Pełne testy bezpieczeństwa dla Web Aplikacji były wykonywane: TAK/NIE
5. Systemy IPS/IDS, Web Application Firewall: TAK/NIE
6. Liczba zewnętrznych adresów IP:
7. Liczba Wewnętrznych adresów IP:
8. Liczba sieci bezprzewodowych WiFi:
9. Web Aplikacja nie wykorzystuje technologii cloud
10. Aplikacja nie posiada obsługi płatności/mikropłatności
11. Web Aplikacja używa zapory znajdującej się w sieci wirtualizacyjnej
12. Ilość zasobów
    a. Serwery (Windows/Linux/Unix)
    b. HyperVisor(vSphere/ESXi, Hyper-V)
    c. Stacje robocze
    d. Inne urządzenia sieciowe

Wymagania konieczne dla wykonawcy:

1. Wykonawca winien wykazać, że dysponuje lub będzie dysponować odpowiednimi zasobami osobowymi o odpowiednich kwalifikacjach:
    a. Co najmniej dwóch audytorów posiadających:
        i. Certyfikaty określone w poniższym wykazie certyfikatów uprawniających do przeprowadzenia audytu lub
        ii. Co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
        iii. Co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych.

2. Wykaz certyfikatów uprawniających do przeprowadzenia audytu:
    a. Certified Internal Auditor (CIA);
    b. Certified Information System Auditor (CISA);
    c. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności I nadzoru rynku, w zakresie certyfikacji osób;

d. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
e. Certified Information Security Manager (CISM);
f. Certified in Risk and Information Systems Control (CRISC);
g. Certified in the Governance of Enterprise IT (CGEIT);
h. Certified Information Systems Security Professional (CISSP);
i. Systems Security Certified Practitioner (SSCP);
j. Certified Reliability Professional;
k. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.