Samodzielny Publiczny Zespół Opieki Zdrowotnej w Sanoku
38-500 Sanok, ul. 800-lecia 26
tel./fax + 48 13 46 56 100
e-mail: szpital@zozsanok.pl, strona : www.zozsanok.pl
NIP 687-16-40-438; REGON 370444345, KRS 0000059726
Dział Zamówień Publicznych
tel. 13/4656290, email: zam.pub@zozsanok.pl

CERTYFIKAT 2022/71

SPZOZ/SAN/ZP/284/2024 Sanok, 02.08.2024 r.

w postępowaniu prowadzonym w trybie zapytania ofertowego na przeprowadzenie ***audytu cyber-bezpieczeństwa. SPZOZ/ZAP/473/2024***

Odpowiedzi na pytania

1. Proszę o informację, czy musi być koniecznie dwóch audytorów wiodących normy ISO 22301 oraz 27001 czy może być to jedna osoba ?

Zamawiający wymaga minimum 2 audytorów posiadających wymienione w zapytaniu uprawnienia zgodnie z wymogiem Ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018 poz. 1560 art. 15. 1 i 2).

2. Ile w sumie organizacja posiada oddziałów lub placówek zamiejscowych, które należy objąć audytem?

Pod głównym adresem znajduje się kilka budynków, dwa kolejne pod innym adresami, wszystkie połączone światłowodem.

3. Adresy utrzymywanych stron www.

www.zozsanok.pl, wyniki.zozsanok.pl

4. Liczba komórek organizacyjnych (działów, departamentów, wydziałów, samodzielnych stanowisk).

14 oddziałów, 6 zakładów, ok. 30 poradni i pracowni, administracja

5. Liczba zatrudnionych osób (w tym pracowników, zleceniobiorców, itp.).

Ok. 900 zatrudnionych.

6. Informacje dotyczące infrastruktury informatycznej, na której przetwarzane są dane (liczba stacji roboczych, serwerów, usług chmurowych itp.)

Ok. 500 stacji roboczych, 25 serwerów

7. Czy i kiedy powołano osobę odpowiedzialną za bezpieczeństwo informacji?

Specjalistę ds. Bezpieczeństwa Informacji powołano w dniu 02.09.2022 r.

8. Informacje na temat dokumentacji związanej z bezpieczeństwem informacji (nazwy dokumentów oraz daty ich ostatniej aktualizacji).

SZBI-001 - Polityka Bezpieczeństwa Informacji - aktualizacja 15.05.2023
SZBI-001-01 - Deklaracja stosowania - aktualizacja 15.05.2023
SZBI-002 - Polityka zarządzania podatnościami - aktualizacja 15.05.2023

SZBI-002-01 - Harmonogram skanowania podatności - aktualizacja 15.05.2023
SZBI-002-02 - Rejestr podatności - aktualizacja 15.05.2023
SZBI-002-03 - Raport podatności - aktualizacja 15.05.2023
SZBI-003 - Polityka ciągłości działania - aktualizacja 15.05.2023
SZBI-003-01 - Plan ciągłości działania - aktualizacja 15.05.2023
SZBI-004 - Polityka bezpieczeństwa fizycznego i środowiskowego - aktualizacja 15.05.2023
SZBI-004-01 - Rejestr gości - aktualizacja 15.05.2023
SZBI-005 - Procedura zarzadzania incydentami - aktualizacja 08.08.2022
SZBI-005-01 - Rejestr incydentów
SZBI-006 - Procedura zarządzania ryzykiem - aktualizacja 08.08.2022
SZBI-006-01 - Klasyfikacja zasobów
SZBI-006-02 - Klasyfikacja zagrożeń
SZBI-006-03 - Analiza Ryzyka - aktualizacja 13.01.2023
SZBI-006-04 - Plan postępowania z ryzykiem
SZBI-007 - Polityka Audytu Wewnętrznego – aktualizacja 15.05.2023
SZBI-007-01 - Harmonogram audytów - aktualizacja 15.05.2023
SZBI-007-02 - Raport z audytu wewnętrznego – aktualizacja 15.05.2023
SZBI-007-03 - Lista kontrolna audytu wewnętrznego - aktualizacja 15.05.2023
SZBI-008 - Instrukcja Zarządzania Systemem Informatycznym - aktualizacja 15.05.2023
SZBI-008-01 - Wniosek o nadanie lub odebranie uprawnień - aktualizacja 01.04.2024
SZBI-008-02 - Ewidencja osób uprawnionych - aktualizacja 15.05.2023
SZBI-008-03 - Harmonogram tworzenia kopii zapasowych - aktualizacja 01.01.2024
SZBI-009 - Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi - aktualizacja 15.05.2023
SZBI-009-01 - Ankieta oceny dostawcy - aktualizacja 15.05.2023

9. Czy w organizacji wdrożono normę ISO 9001 lub ISO 27001 bądź inną?

Wdrożono iso 27001 – bez certyfikacji.

Pytania do przeprowadzenia testów penetracyjnych:

Audyt bezpieczeństwa infrastruktury:

10. Jakie są oczekiwania Zamawiającego odnośnie do ilości systemów, które powinny zostać poddane analizie w ramach audytu bezpieczeństwa?

Zapora sieciowa, system kopii zapasowej, sieć wewnętrzna – serwerowa, SIEM/SOAR.

11. Jaki ma być zakres testów penetracyjnych infrastruktury? (np. czy w ramach testów ma zostać zweryfikowana sieć serwerowa, czy również część przeznaczona dla użytkowników?)

Sieć wewnętrzna – serwerowa.

12. Jaka jest całościowa ilość adresów IP podlegająca audytowi bezpieczeństwa?

Wszystkie hosty, od 800-900 adresów.

13. Ile Zamawiający posiada łącznie systemów i aplikacji, które będą podlegać audytowi?

Zapora sieciowa, system kopii zapasowej, sieć wewnętrzna – serwerowa, SIEM/SOAR.

14. W oparciu o jakie technologie funkcjonuje infrastruktura systemu (systemy operacyjne, bazy danych, aplikacje, moduły komunikacji)?

Ze względów bezpieczeństwa Zamawiający udzieli powyższej informacji wyłonionemu Wykonawcy przedmiotu zamówienia.

15. Ile jest podsieci?

9 VLAN

16. Ile jest aktywnych host'ów w podsieciach?

Ok. 950 hostów

17. Czy dostęp jest z Internetu czy tylko przez VPN?

Dostęp z zewnątrz realizowany jest zarówno z wykorzystaniem VPN oraz z sieci Internet.

18. Jakie adresy dostępne są z Internetu? Ile jest takich adresów IP?

3 adresy IP dostępne z sieci Internet.

19. Ile Zamawiający posiada lokalizacji?

Pod głównym adresem znajduje się kilka budynków, dwa kolejne pod innym adresami, wszystkie połączone światłowodem.

20. Czy Zamawiający ma wdrożoną usługę katalogową Active Directory lub inną?

Tak.

21. Czy Zamawiający ma wdrożony proces zarządzania podatnościami oparty o zautomatyzowane narzędzia (np. Nessus, Nexpose, Qualys lub inne)?

Zamawiający ma wdrożony proces zarządzania podatnościami oparty o zautomatyzowane narzędzia.

22. Kiedy powinien rozpocząć się audyt bezpieczeństwa?

Można rozpocząć prace bezpośrednio po podpisaniu umowy.

23. Czy w zakresie audytu powinien znajdować się również przeprowadzenie retestu zidentyfikowanych podatności?

Tak.

24. Na kiedy najpóźniej powinien zostać dostarczony raport i w jakim/jakich językach?

Raporty w języku polskim (papierowo i elektronicznie), terminy podane są w umowie.

25. Czy audyt może być wykonywany zdalnie?

Wymaga się aby audyt został przeprowadzony w siedzibie Zamawiającego. Zmieniono zapisy umowy.

<u>Audyt Wifi:</u>

26. Jaka jest szacowana ilość urządzeń sieciowych będących w zakresie przeglądu konfiguracji (w podziale na urządzenia typu Access Point, Network Controller, IPS, Firewall)?

Sieć wifi nie podlega audytowi.

27. W oparciu o jakie rozwiązania zbudowana jest sieć bezprzewodowa (producent, typ, wersja)?

Sieć wifi nie podlega audytowi.

28. Czy istnieje dokumentacja dotycząca budowy sieci bezprzewodowych?

Sieć wifi nie podlega audytowi.

29. W ilu lokalizacjach mają zostać przeprowadzone testy sieci WiFi? Jaki jest rozmiar tych lokalizacji (liczba pięter)?

Sieć wifi nie podlega audytowi.

30. Czy będzie istniała możliwość przekazania materiałów do analizy (konfiguracji) na stacje robocze audytora, czy też prace będą musiały być realizowane w Państwa siedzibie?

Wymaga się aby audyt został przeprowadzony w siedzibie Zamawiającego. Zmieniono zapisy umowy.

31. Ile sieci należących do Państwa ma zostać poddanych badaniu? Jakie to sieci (np. firmowa, dla gości)?

Sieć wifi nie podlega audytowi.

32. Czy prace mają objąć zakresem analizy wyłącznie sieci WiFi, czy też komunikacja działająca w obszarze całego widma bezprzewodowego w siedzibie?

Sieć wifi nie podlega audytowi.

33. Czy w ramach prac ma zostać przeprowadzona analiza istniejącego środowiska bezprzewodowego pod kątem istnienia nieautoryzowanych Access Point-ów?

Sieć wifi nie podlega audytowi.

34. Czy testy sieci WiFi mają obejmować swoim zakresem również przegląd konfiguracji wybranych elementów infrastruktury wspierającej? Jeżeli tak, to jakie i ile konfiguracji jest w zakresie prac?

Sieć wifi nie podlega audytowi.

35. Czy w zakresie analizy jest również weryfikacja sieci, do których łączą się pracownicy firmy?

Sieć wifi nie podlega audytowi.

36. Czy w ramach prac mają zostać przeprowadzona próby ataków na użytkowników Państwa organizacji poprzez stworzenie nieautoryzowanej sieci bezprzewodowej i analizę ruchu w sieci?

Sieć wifi nie podlega audytowi.

37. Czy w zakresie prac znajduje się również identyfikacja realizowanych ataków na Państwa sieci bezprzewodowe?

Sieć wifi nie podlega audytowi.

<u>Testy penetracyjne aplikacji:</u>

38. Czy do wykonania będzie black/grey/white – box. Czy otrzymamy dostęp do zalogowania się do web/mobile aplikacji?

Metodyka: grey box, maksymalnie do 5 aplikacji wybranych po wykonaniu skanu wspólnie z Zamawiającym.

a) Ile i jakie aplikacje mają zostać przetestowane?

Maksymalnie do 5 aplikacji wybranych po wykonaniu skanu wspólnie z Zamawiającym.

b) Ilość systemów

Maksymalnie do 5 aplikacji wybranych po wykonaniu skanu wspólnie z Zamawiającym.

c) Nazwy i wersje poszczególnych komponentów (front'end / backend / bazy danych)

Ze względów bezpieczeństwa Zamawiający udzieli powyższej informacji wyłonionemu Wykonawcy przedmiotu zamówienia.

d) Lokalizacja portali (wewnętrzne / zewnętrzne)

Wszelkie aplikacje poddane audytowi działają na serwerach Zamawiającego

39. Jaka jest szacowana wielkość webaplikacji/portali? – poniżej pytania per aplikacja:

Ze względów bezpieczeństwa Zamawiający udzieli powyższej informacji wyłonionemu Wykonawcy przedmiotu zamówienia.

a) Czy aplikacja posiada tryb rejestracji, logowania i tworzenia profili?
b) Czy aplikacja wymaga rejestracji użytkowników?
c) Czy użytkownicy posiadający tę samą rolę mają dostęp do tego samego zestawu danych?
d) Prosimy o wskazanie krótkiego opisu każdej roli użytkownika zaimplementowanej w aplikacji.
e) Czy aplikacja posiada funkcję załączania plików na serwer? Jeśli tak, ile jest miejsc w aplikacji, które pozwalają na załączanie plików?
f) Jakie dane będą przetwarzane przez aplikację?
g) Ile podstron zawierać będzie aplikacja?
h) Ile formularzy zawierać będzie aplikacja?
i) Ile jest poziomów użytkowników? (administrator, użytkownik uprzywilejowany, normalny użytkownik, inne)
j) Czy systemy są chronione przez FW warstwy 7-mej (WAF)?

Ze względów bezpieczeństwa Zamawiający udzieli powyższej informacji wyłonionemu Wykonawcy przedmiotu zamówienia.

k) Czy są wykorzystywane rozwiązania chmurowe (ze szczególnym uwzględnieniem rozwiązań PaaS)?

Zakres prac nie będzie obejmować rozwiązań chmurowych.

l) Kiedy powinny rozpocząć się testy penetracyjne?

Można rozpocząć prace bezpośrednio po podpisaniu umowy.

m) Na kiedy najpóźniej powinien zostać dostarczony raport i w jakim/jakich językach?

W języku polskim do końca września 2024 roku.

n) W jakich godzinach mogą być wykonywane testy penetracyjne?

W godz. 7.30 do 14.30.

Z poważaniem

DYREKTOR
SPZOZ w Sanoku
mgr Grzegorz Panek, MBA