Włocławek, dnia 02.12.2024r.

G.231.393.2024

W ramach postępowania na *„Wykonanie audytu cyberbezpieczeństwa wraz
z audytem zgodności z dyrektywą NIS2 dla Państwowej Akademii Nauk Stosowanych we Włocławku”* do Zamawiającego wpłynęły następujące pytania na które zostały udzielone niniejsze odpowiedzi:

Audyt bezpieczeństwa infrastruktury:
Pyt. 1. Jakie są oczekiwania Zamawiającego odnośnie ilości systemów, które powinny zostać poddane analizie w ramach audytu bezpieczeństwa?

Odp.1. 3 kluczowe systemy tj. kadrowo-finansowy + biblioteczny + system do zarządzania Uczelnią

Pyt. 2. Jaki ma być zakres testów penetracyjnych infrastruktury?
(np. czy w ramach testów ma zostać zweryfikowana sieć serwerowa, czy również część przeznaczona dla użytkowników?)

Odp. 2. Jeden VLAN tzw. administracyjny około 80 jednostek

Pyt 3. Jaka jest całościowa ilość adresów IP podlegająca audytowi bezpieczeństwa?

Odp. 3. około 80 jednostek

Pyt. 4. Ile Zamawiający posiada łącznie systemów i aplikacji, które będą podlegać audytowi?

Odp. 4. 3 kluczowe systemy + kilka mniej istotnych + strony www

Pyt. 5. W oparciu o jakie technologie funkcjonuje infrastruktura systemu (systemy operacyjne, bazy danych, aplikacje, moduły komunikacji)?

Odp. 5. Windows, linux, MS SQL itp.

Pyt. 6. Ile jest podsieci?

Odp. 6. Audyt dotyczy jednej podsieci

Pyt. 7. Ile jest aktywnych host’ów w podsieciach?

Odp. 7. Audyt dotyczy jednej podsieci, około 80

Pyt. 8. Czy dostęp jest z Internetu czy tylko przez VPN?

Odp. 8. Obydwa powyższe

Pyt. 9. Jakie adresy dostępne są z Internetu? Ile jest takich adresów IP?

Odp. 9. Linki do usług można znaleźć na uczelnianej stronie www.pans.wloclawek.pl

Pyt. 10. Ile Zamawiający posiada lokalizacji?

Odp. 10. <https://pans.wloclawek.pl/baza-dydaktyczna/>

Pyt. 11. Czy Zamawiający ma wdrożoną usługę katalogową Active Directory lub inną?

Odp. 11. W sieci, która będzie audytowana nie

Pyt. 12. Czy Zamawiający ma wdrożony proces zarządzania podatnościami oparty o zautomatyzowane narzędzia (np. Nessus, Nexpose, Qualys lub inne)?

Odp. 12. Zostanie to omówione dokładnie podczas pierwszych spotkań z wyłonionym Wykonawcą.

Pyt.13. Kiedy powinien rozpocząć się audyt bezpieczeństwa?

Odop. 3. Zostało to opisane w dokumentacji zapytania ofertowego.

Pyt. 14. Czy w zakresie audytu powinien znajdować się również przeprowadzenie retestu zidentyfikowanych podatności?

Odp. 14. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Pyt. 15. Na kiedy najpóźniej powinien zostać dostarczony raport
i w jakim/jakich językach?

Odp. 15. Zostało to opisane w dokumentacji zapytania ofertowego/w języku polski.

Pyt. 16. Czy audyt może być wykonywany zdalnie?

Odp. 16. Zostało to opisane w dokumentacji zapytania ofertowego.

Audyt systemu:
Pyt. 1. Jaki jest oczekiwany zakres prac (np. testy penetracyjne aplikacji oraz infrastruktury, analiza konfiguracji infrastruktury, analiza otoczenia sieciowego systemu, itp.)?

Odp. 1. Tak, powyższe.

Pyt. 2. Czy prace w ramach mają zostać przeprowadzone zarówno w warstwie technicznej (przegląd konfiguracji systemów), jak i w warstwie procesowej?

Odp. 2. Tak, powyższe.

Pyt. 3. Czy procesy zarządzania systemami są spójne dla systemów w zakresie prac?

Odp. 3. Tak są spójne

Pyt. 4. Jakie są oczekiwania odnośnie ilości systemów, które powinny zostać poddane analizie w ramach prac?

Odp. 4. 3 kluczowe systemy + kilka mniej istotnych + strony www

Pyt. 5. Czy oprócz przedmiotowego rozwiązania zakresem audytu będą jeszcze inne elementy infrastruktury wspierającej system? Jeżeli tak to jakie?

Odp. 5. Zostało to opisane w dokumentacji zapytania ofertowego.

Pyt. 6. W oparciu o jakie technologie funkcjonuje infrastruktura systemu (system operacyjny, baza danych, aplikacje, moduły komunikacji, ile urządzeń/systemów będzie podlegać audytowi (per typ urządzenia)?

Odp. 6. Zostanie to omówione dokładnie podczas pierwszych spotkań z wyłonionym Wykonawcą, około 80 jednostek

Pyt. 7. Jaki urządzenia sieciowe będą podlegały przeglądowi konfiguracji (producent, typ)?

Odp. 7. Zostanie to omówione dokładnie podczas pierwszych spotkań z wyłonionym Wykonawcą.

Pyt. 8. W jakiej lokalizacji będą prowadzone prace?

Odp. 8. <https://pans.wloclawek.pl/baza-dydaktyczna/>

Pyt. 9. Czy będzie istniała możliwość przekazania materiałów do analizy na stacje robocze audytora?

Odp. 9. Tak jeśli przygotowanie tych materiałów nie narazi Zamawiającego na dużo większy zakres prac niż by to było wykonane metodą tradycyjną.

Pyt. 10. Czy w zakresie audytu znajduje się również przeprowadzenie retestu zidentyfikowanych podatności?

Odp. 10. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Audyt Wifi:
Pyt. 1. Jaka jest szacowana ilość urządzeń sieciowych będących w zakresie przeglądu konfiguracji (w podziale na urządzenia typu Access Point, Network Controller, IPS, Firewall)?

Odp. 1. Około 8 urządzeń

Pyt.2. W oparciu o jakie rozwiązania zbudowana jest sieć bezprzewodowa (producent, typ, wersja)?

Odp.2. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Pyt. 3. Czy istnieje dokumentacja dotycząca budowy sieci bezprzewodowych?

Odp. 3. Nie

Pyt. 4. W ilu lokalizacjach mają zostać przeprowadzone testy sieci WiFi? Jaki jest rozmiar tych lokalizacji (liczba pięter)?

Odp. 4. <https://pans.wloclawek.pl/baza-dydaktyczna/>

Pyt. 5. Czy będzie istniała możliwość przekazania materiałów do analizy (konfiguracji) na stacje robocze audytora, czy też prace będą musiały być realizowane w Państwa siedzibie?

Odp. 5. Tak jeśli przygotowanie tych materiałów nie narazi Zamawiającego na dużo większy zakres prac niż by to było wykonane metodą tradycyjną

Pyt. 6. Ile sieci należących do Państwa ma zostać poddanych badaniu? Jakie to sieci (np. firmowa, dla gości)?

Odp. 6. Jeden VLAN tzw. administracyjny około 80 jednostek

Pyt. 7. Czy prace mają objąć zakresem analizy wyłącznie sieci WiFi, czy też komunikacja działająca w obszarze całego widma bezprzewodowego w siedzibie?

Odp. 7. Wyłącznie sieci WiFi

Pyt. 8. Czy w ramach prac ma zostać przeprowadzona analiza isntniejącego środowiska bezprzewodowego pod kątem istnienia nieautoryzowanych Access Point-ów?

Odp. 8. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Pyt. 9. 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?

Odp.9. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Pyt. 10. Czy w zakresie analizy jest również weryfikacja sieci, do których łączą się pracownicy firmy?

Odp. 10. Pracownicy łączą się tylko z jedną siecią.

Pyt. 11. Czy w ramach prac mają zostać przeprowadzona próby ataków na użytkowników Państwa organizacji poprzez stworzenie nieautoryzowanej sieci bezprzewodowej i analizę ruchu w sieci?

Odp. 11. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Pyt. 12. Czy w zakresie prac znajduje się również identyfikacja realizowanych ataków na Państwa sieci bezprzewodowe?

Odp. 12. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.

Testy penetracyjne aplikacji:
Pyt. 1. Czy do wykonania będzie black/grey/white – box. Czy otrzymamy dostęp do zalogowania się do web/mobile aplikacji?
a. Ile i jakie aplikacje mają zostać przetestowane?

Odp. 1a. 3 kluczowe systemy + kilka mniej istotnych + strony www. Linki do wszystkich stron uczelni można znaleźć na uczelnianej stronie www.pans.wloclawek.pl

Zostanie to omówione dokładnie podczas pierwszych spotkań z wyłonionym Wykonawcą. Szczegółowe dane o systemach i ich konfiguracji, uważamy, że nie powinny zostać podawane do informacji publicznej.
i. Ilość systemów;
ii. Nazwy i wersje poszczególnych komponentów (front’end / backend / bazy danych)
iii. Lokalizacja portali (wewnętrzne / zewnętrzne)
iv. Jaka jest szacowana wielkość webaplikacji/portali? – poniżej pytania per aplikacja:
1. Czy aplikacja posiada tryb rejestracji, logowania
i tworzenia profili?
2. Czy aplikacja wymaga rejestracji użytkowników?
3. Czy użytkownicy posiadający tę samą rolę mają dostęp do tego samego zestawu danych?
4. Prosimy o wskazanie krótkiego opisu każdej roli użytkownika zaimplementowanej w aplikacji.
5. Czy aplikacja posiada funkcję załączania plików na serwer? Jeśli tak, ile jest miejsc w aplikacji, które pozwalają na załączanie plików?
6. Jakie dane będą przetwarzane przez aplikację?
7. Ile podstron zawierać będzie aplikacja?
8. Ile formularzy zawierać będzie aplikacja?
9. Ile jest poziomów użytkowników? (administrator, użytkownik uprzywilejowany, normalny użytkownik, inne)

Pyt. 2. Czy systemy są chronione przez FW warstwy 7-mej (WAF)?

Odp. 2. Zostanie to omówione dokładnie podczas pierwszych spotkań z wyłonionym Wykonawcą. Szczegółowe dane o systemach uważamy, że nie powinny zostać podawane do informacji publicznej.

Pyt. 3. Czy są wykorzystywane rozwiązania chmurowe (ze szczególnym uwzględnieniem rozwiązań PaaS)?

Odp.3. Tak są

Pyt. 4. Kiedy powinny rozpocząć się testy penetracyjne?

Odp.4. Zostało to opisane

Pyt. 5. Na kiedy najpóźniej powinien zostać dostarczony raport i w jakim/jakich językach?

Odp. 5. Zostało to opisane, język polski.

Pyt. 6. W jakich godzinach mogą być wykonywane testy penetracyjne?

Odp. 6. To zależy od wykonawcy. Jakie ma metody przeprowadzania audytu.