Załącznik do zawiadomienia
z dnia 20 czerwca 2022r.

Pytania i Odpowiedzi do Zapytania Ofertowego na realizację zamówienia pn.:
„USŁUGA PRZEPROWADZENIA DIAGNOZY CYBERBEZPIECZEŃSTWA W URZĘDZIE GMINY WARTKOWICE"
z dnia 09 czerwca 2022r.

ODPOWIEDZI NA ŻÓŁTYM TLE

1. Lokalizacja jednostek audytowanych (adresy, inf. co znajduje się pod danym adresem)

   Pozostałe dane poniżej proszę rozgraniczyć na <u>każdą jednostkę z osobna</u>, pozwoli to najdokładniej obliczyć czasochłonność i cenę projektu:

   Urząd Gminy Wartkowice Stary Gostków 3D 99-220 Wartkowice

2. Ilość pracowników/użytkowników
   24
3. Ilość <u>wszystkich hostów</u> podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.). W tym rozgraniczyć:
   a. Ilość komputerów (również przenośnych) 26
   b. Ilość serwerów (fizycznych, wirtualnych) 2/2
   c. Ilość pozostałych urządzeń podłączonych do sieci 37 – w tym 25 telefonów IP.
4. Ilość podsieci 2
5. Ilość serwerowni 2
6. Ilość adresów zewnętrznych 1
7. Czy mają Państwo wdrożoną Active Directory? Tak
8. Jaki budżet (brutto) wpisali Państwo we wniosku grantowym na realizację samej Diagnozy cyberbezpieczeństwa z całej puli przydzielonych środków?
   Zawarte w dwóch pozycjach:
   Diagnoza cyberbezpieczeństwa – 9225 PLN
   Przeprowadzenie audytu bezpieczeństwa informacji zgodnie z KRI oraz wdrożenie SZBI – 17220 PLN

9. Punkt 2.8 - *Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe*
   Mają być przeprowadzone testy odtworzeniowe, czy ma być oceniony na zasadzie audytu proces archiwizacji i stwierdzenie, czy testy są robione czy nie, poprawność procesu itp.?

   Można zapisać jak poniżej bardziej szczegółowo.

   Propozycja zmiany w tym punkcie:

2.8. Analiza i ocena systemów backupów i archiwizacji danych w tym testy odtworzeniowe

2.8.1. Weryfikacja i ocena procedur wykonywania kopii zapasowych zawartych w dokumentacji bezpieczeństwa

2.8.2. Weryfikacja i ocena wykazów, logów świadczących o realizacji zadań zgodnie z przyjętymi zapisami w polityce

2.8.3. Weryfikacja zasobów do wykonywania testów odtworzeniowych

2.8.4. Weryfikacja czy są wykonywane testowe odtworzenia

10. Proponujemy rozszerzenie punktu 2.10 - *Testy penetracyjne systemów informatycznych i całej infrastruktury ICT*:

25Proponujemy wstawienie szerszego zakresu testów punktu 2.10 odnośnie testów penetracyjnych i usunięcie kilku punktów z obecnego zakresu, które się w testach zawierają, żeby się nie dublowały. Proponowany zakres testów:

1. Testy penetracyjne systemów informatycznych i całej infrastruktury ICT
   1.1. Testy styku sieci lokalnej z Internetem przeprowadzane ze stacji roboczej podłączonej do sieci Internet
   - Analiza topologii brzegu sieci
   - Weryfikacja mechanizmów ochronnych
   - Próba wykrycia usług sieciowych udostępnianych do Internetu
   - Detekcja wersji oraz typu oprogramowania dostępnego z sieci Internet
   - Exploitacja dostępnych urządzeń oraz usług wystawionych do sieci Internet
   - Przedstawienie rozwiązań zwiększających bezpieczeństw styku sieci lokalnej z siecią Internet

   1.2. Testy penetracyjne przeprowadzone ze stacji roboczej podłączonej do wewnętrznego systemu informatycznego w celu zidentyfikowania możliwości przeprowadzenia włamania z wewnątrz organizacji
   - Analiza topologii sieci LAN
   - Weryfikacja mechanizmów ochronnych w sieci
   - Analiza komunikacji sieciowe
   - Skanowanie portów TCP/UDP próba wykrycia usług sieciowych
   - Skanowanie hostów aktywnych w sieci
   - Exploitacja dostępnych urządzeń oraz usług w sieci LAN
   - Przedstawienie rozwiązań zwiększających bezpieczeństw sieci LAN

Można zapisać jak powyżej bardziej szczegółowo.

11. Punkty 2.12 - *Badanie podatności usług sieciowych* oraz 2.13 - *Badanie podatności aplikacji serwera pocztowego email i aplikacji webowej zgodnie z OWASP* — do usunięcia, jeżeli powyższy zakres Testów penetracyjnych zostanie przez Państwa uznany – te punkty będą zawierały się w punkcie 2.10 w zakresie pełnych testów penetracyjnych.

Do usunięcia.

12. Punkt 2.17 - *Sprawdzenie i ocena szyfrowania danych przechowywanych poza Urzędem m.in. serwisy pocztowe email, serwisy WEB itp.* – do usunięcia, nie leży to w gestii firmy audytorskiej, do zweryfikowania między Urzędem a dostawcą, stroną trzecią.

Podlega sprawdzeniu.

13. Punkt 2.11 oraz 2.18 dot. *sprawdzeń przed atakami pishingowymi* – czy chodzi Państwu o przeprowadzenie takich ataków socjotechnicznych?

Przeprowadzić test najlepiej przed szkoleniem pracowników..

14. Punkt 2.20 - *Identyfikacja pojedynczych punktów awarii* – do usunięcia, raczej nie robi się tego podczas audytu.

Do usunięcia – ale miejsca potencjalnych awarii i ich skutków muszą być zawarte w dokumentacji analizy ryzyka

15. Punkt 3.9 - *Rozpoznanie wszystkich systemów przetwarzających dane i ich konfigurację* - Trochę niejasny punkt i wydający się zbyt ogólnie napisany. Domyślamy się, że odpowiedzi na to znajdą się po przeprowadzeniu testów i ocenie haseł. Punkt raczej do usunięcia, zdubluje już wcześniej zapisane odnośnie audytu ODO.

Do usunięcia.

16. Punkt 3.10 - *Rozpoznanie wszystkich przetwarzanych zbiorów danych* - Potrzebna zmiana na analizę lub przegląd procesów przetwarzania danych osobowych. Zbiory danych już dawno nie istnieją i odnoszą się do starych przepisów przed wejściem RODO.

Do usunięcia.

17. Punkty 3.11 i 3.12 oraz 3.15 – do usunięcia, odnoszą się do starych przepisów przed wejściem RODO.

Do usunięcia.

18. Punkt 3.16 oraz 3.17 – do usunięcie, niepotrzebne wyszczególnienia i powielanie, tych punktów dotyczy cały audyt ODO opisany we wcześniejszych punktach.

Do usunięcia.

19. Punkt 3.20 - *Analiza i ocena zaangażowania Najwyższego Kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji* – punkt odnoszący się głębiej do ISO, niepotrzebny na poziomie SZBI opartego na KRI w Urzędzie. Do usunięcia.

Do usunięcia

20. Punkt 3.30 - *Analiza i ocena stron webowych pod kątem zgodności standardu min. WCAG 2.1* – Całkiem niedawno wchodziła nowa ustawa w związku z dostępnością, czy nie robili Państwo takiego audytu? Jeżeli Państwu zależy na przeprowadzeniu tego to proszę podać jakie adresy www miałyby być sprawdzone.
Z punktu widzenia SZBI taki audyt nie jest niezbędny a wygeneruje spore dodatkowe koszty.

Do pominięcia w analizie cyberbezpieczeństwa

21. Wynikiem audytu ma być „opracowanie i wdrożenie SZBI" – proszę o sprezycowanie czy chodzi Państwu o aktualizację podstawowych polityk typu polityka bezpieczeństwa informacji, ochrony danych osobowych, instrukcja zarządzania systemami informatycznymi itp. dokumenty czy coś innego?

Ma być stworzona kompletna dokumentacja i opracowanie wszystkich polityk bezpieczeństwa

22. Odnosząc się do treści zał. 8 konkursu zawartej w arkuszu CERT (punkty od 3 do 6 włącznie), proszę o informacje czy posiadają Państwo Dokumentację oraz Raporty/Wyniki z audytów tam wskazane, aby było możliwe ich sprawdzenie/ocena podczas Diagnozy? Czy oczekują Państwo wykonania podczas Diagnozy któregokolwiek z tych audytów lub opracowania dokumentacji – jeśli tak proszę o wskazanie konkretnych punktów z arkusza CERT, które ma opracować Wykonawca i uwzględnić taką informację jako oficjalną zmianę w treści zapytania. Poniżej lista z załącznika nr 8 konkursu (proszę o wpisanie czy Urząd posiada daną dokumentację, raporty lub czy wymaga jej ewentualnego opracowania):

3	**Dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne**	**Tak**	**Nie**	**Opracowuje Wykonawca**
3.1	Czy istnieją raporty z audytów systemów informacyjnych wspierających zadanie publiczne?			Opracowuje Wykonawca
3.2	Czy istnieje dokumentacja architektury zastosowanych zabezpieczeń?			Opracowuje Wykonawca
3.3	Czy istnieje dokumentacja architektury sieci?			Opracowuje Wykonawca
3.4	Czy istnieje baza danych konfiguracji urządzeń aktywnych?			Opracowuje Wykonawca
3.5	Czy istnieje dokumentacja zmian w systemach informacyjnych?			Opracowuje Wykonawca
3.6	Czy istnieje dokumentacja dotycząca monitorowania w trybie ciągłym?			Opracowuje Wykonawca
3.7	Czy są dostępne umowy z dostawcami (wsparcie techniczne)?			Opracowuje Wykonawca
3.8	Czy są zawierane umowy z dostawcami usług z zakresu bezpieczeństwa teleinformatycznego?			Opracowuje Wykonawca
3.9	Czy są wymagane wyniki audytów u dostawców usług bezpieczeństwa teleinformatycznego?			Opracowuje Wykonawca
3.10	Czy jest dostępna i aktualna dokumentacja zabezpieczeń fizycznych i środowiskowych?			Opracowuje Wykonawca
3.11	Czy jest prowadzony rejestr dostępu do dokumentacji systemu informacyjnego?			Opracowuje Wykonawca
4	**Dokumentacja procesu zarządzania incydentami**			
4.2	Czy istnieje procedura informowania o wykrytych incydentach?			Opracowuje Wykonawca
4.3	Czy istnieją procedury reagowania na incydenty?			Opracowuje Wykonawca
5	**Aspekty techniczne do weryfikacji**			

5.1	Wyniki audytu serwisów WWW z uwzględnieniem: - wersji serwera HTTP; - wersji systemu CMS (o ile występuje); - bezpieczeństwa komunikacji (aktualność certyfikatów X.509, wersja TLS, stosowane algorytmy kryptograficzne itp.); - dostępności kompetentnego personelu do utrzymania serwisów.			Opracowuje Wykonawca
5.2	Wyniki audytu serwisów pocztowych z uwzględnieniem: - poprawności wdrożenia mechanizmów SPF, DKIM i DMARC; - poprawności i bezpieczeństwa wdrożenia mechanizmów TLS; - dostępności kompetentnego personelu do utrzymania serwisów.			Opracowuje Wykonawca
5.3	Wyniki audytu lokalnych sieci teleinformatycznych z uwzględnieniem: - wdrożenia systemów ochrony przed kodem szkodliwym w sposób zapewniający ich automatyczną aktualizację; - stosowania mechanizmów segmentacji sieci; - izolacji urządzeń końcowych użytkowników; - procesu tworzenia i okresowego odtwarzania kopii zapasowych przetwarzanych informacji; - monitorowania ruchu wewnątrz sieci w zakresie wykrywania symptomów naruszeń bezpieczeństwa; - dostępności kompetentnego personelu do utrzymania infrastruktury sieciowej.			Opracowuje Wykonawca
5.4	Wyniki audytu połączenia z siecią Internet z uwzględnieniem: - monitorowania ruchu wchodzącego i wychodzącego; - stosowanych zabezpieczeń przed atakami DDoS; - stosowanych zabezpieczeń przed wyciekiem informacji (DLP); - stosowanych zabezpieczeń punktu styku (FW, IDS, IPS, WAF itp.); - dostępności kompetentnego personelu do utrzymania punktu styku z siecią Internet.			Opracowuje Wykonawca
6	**Aspekty organizacyjne do weryfikacji**			
6.1	Wyniki audytu organizacji zarządzania bezpieczeństwem teleinformatycznym z uwzględnieniem: - regularnego identyfikowania znanych podatności w eksploatowanych systemach IT; - terminowego wprowadzania danych do systemów zarządzania tożsamością i uprawnieniami użytkowników; - prowadzenia okresowego przeglądu uprawnień użytkowników; - prowadzenia okresowych szkoleń użytkowników podnoszących ich świadomość zagrożeń.			Opracowuje Wykonawca
6.2	Wyniki audytu procesów planowania z uwzględnieniem: - posiadania planów przywracania usług IT na wypadek awarii; - prowadzenia przeglądów oraz doskonalenia planów przywracania usług IT; - cyklu życia systemów IT i eksploatacji produktów nieposiadających wsparcia producenta.			Opracowuje Wykonawca

Sporządził: Rafał Prośniak