GŁÓWNY INSPEKTORAT TRANSPORTUDROGOWEGO

Warszawa, dnia 17.09.2024r.

Do wykonawców w postępowaniu

Dotyczy: postępowania o udzielenie zamówienia publicznego bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605) prowadzone w formie zapytania ofertowego którego przedmiotem jest:
„Przeprowadzenie testów penetracyjnych w siedzibach Głównego Inspektoratu Transportu Drogowego"

Zamawiający - Skarb Państwa - Główny Inspektorat Transportu Drogowego udziela odpowiedzi na pytania wniesione przez Wykonawców:

Pytanie nr 1:

2.1.1.6. Analiza konfiguracji serwerów webowych. ->Jaka jest ilość serwerów podlegających badaniu konfiguracji, wchodzących w skład infrastruktury badanych 2 aplikacji? Jakie są role badanych serwerów? Czy Zamawiający poprzez "analiza konfiguracji" rozumie analizę plików konfiguracyjnych usług świadczonych przez te serwery?

Odpowiedź nr 1:

a. Liczba serwerów aplikacyjnych będących przedmiotem badania wynosi 4.
b. Role badanych serwerów są następujące: serwery aplikacyjne i serwery bazodanowe.
c. Zamawiający rozumie tutaj analizę podatności oprogramowania.

Pytanie nr 2:

2.2.1.3. Testy odporności na ataki DoS/DDoS wolumetryczne oraz aplikacyjne ->Jaka jest ilość aplikacji, ilość serwerów bądź adresów IP podlegających badaniu?

Odpowiedź nr 2:

Zamawiający posiada dwie klasy adresów z maską 24. Po podpisaniu umowy wskaże po 3 adresy IP z każdej z klas.

Pytanie nr 3:

2.2.1.5. Sprawdzenie polityk zabezpieczeń sieci. (w zakresie podłączania obcych urządzeń, przechodzenia między podsieciami, separacji logicznej sieci itp.) ->Jaka jest ilość urządzeń podlegających pod weryfikację polityk? Rodzaje oraz role tych urządzeń.

Czy Zamawiający rozumie weryfikacje polityk jako sprawdzenie konfiguracji badanego urządzenia?

Odpowiedź nr 3:

Liczba urządzeń podlegających pod weryfikację polityk wynosi 2 UTM.
Zamawiający rozumie tu sprawdzenie pod kątem podatności badanego urządzenia.

Pytanie nr 4:

2.3.1.1. Analizę konfiguracji serwerów pod kątem bezpieczeństwa – > Czy Zamawiający rozumie przez analizę konfiguracji systemu weryfikacje na zgodność z best practices lub CIS Benchmarks?

Odpowiedź nr 4:

Zamawiający rozumie tutaj analizę podatności oprogramowania.

Pytanie nr 5:

2.3.1.2. Analiza bezpieczeństwa Active Directory ->Czy Zamawiający rozumie przez to analizę konfiguracji systemu na zgodność z best practices lub CIS Benchmarks?

Odpowiedź nr 5:

Zamawiający rozumie tutaj weryfikację podatności na aktualne zagrożenia.

Pytanie nr 6:

2.3.1.5. Sprawdzenie polityk zarządzania użytkownikami i kontrolą dostępu. ->Czy Zamawiający rozumie przez to analizę konfiguracji systemu na zgodność z best practices lub CIS Benchmarks?

Odpowiedź nr 6:

Zamawiający rozumie tutaj weryfikację podatności typu eskalacja uprawnień.

Pytanie nr 7:

2.3.1.6. Weryfikacja kont z dostępem administracyjnym i zakresu dostępów. ->Czy Zamawiający rozumie przez to analizę konfiguracji systemu na zgodność z best practises lub CIS Benchmarks?

Odpowiedź nr 7:

Zamawiający rozumie tutaj weryfikację podatności typu eskalacja uprawnień.

Pytanie nr 8:

2.3.1.8. Analiza i testy zabezpieczeń baz danych. ->Czy Zamawiający rozumie przez to analizę konfiguracji systemu na zgodność z best practices lub CIS Benchmarks?

Odpowiedź nr 8:

Zamawiający oczekuje weryfikacji serwerów bazodanowych w ramach weryfikacji aplikacji webowych pod kątem zagrożeń z listy OWASP TOP10.

Pytanie nr 9:

2.3.1.9. Weryfikacja poprawności stosowania aktualizacji i łat bezpieczeństwa. ->Czy Zamawiający rozumie przez to analizę konfiguracji systemu na zgodność z best practices lub CIS Benchmarks?

Odpowiedź nr 9:

Zamawiający rozumie tutaj weryfikację podatności na aktualne zagrożenia.

Pytanie nr 10:

2.3.1.10. Testy systemów kopii zapasowych i odzyskiwania danych. ->Czy Zamawiający przewiduje podczas testów przeprowadzenia kopii systemu i weryfikacje poprzez jej odtworzenie?

Odpowiedź nr 10:

Tak, dla jednego wybranego serwera.

Pytanie nr 11:

Ad. 2.3 Czy zmawiający w ramach badania infrastruktury serwerowej ma na myśli weryfikacje konfiguracji serwerów?

Odpowiedź nr 11:

Zamawiający rozumie tutaj weryfikację podatności na aktualne zagrożenia.

Pytanie nr 12:

2.4.1.2. Różne scenariusze ataków, zaproponowane przez Wykonawcę ->Jaka jest oczekiwana liczba scenariuszy? Jaką ilość scenariuszy Zamawiający oczekuje wykonać na grupie 100 adresów? Czy wszyscy adresaci mają zostać objęci tymi samymi scenariuszami? Czy wskazane grupy wskazanymi scenariuszami?

Odpowiedź nr 12:

Minimum 2 scenariusze. Wszyscy adresaci musza zostać objęci tymi scenariuszami.

Pytanie nr 13.1:

Pytania odnośnie punktu 2.2.1.3. OPZ - Testy odporności na ataki DoS/DDoS :

1. Ile publicznych adresów IP ma podlegać atakowi?

Odpowiedź nr 13.1:

Patrz odpowiedź z pytanie nr 2:

Pytanie nr 13.2:

2. Jaki jest oczekiwany wolumen ruchu (np. 100Mbps, 500Mbps,1Gbits)?

Odpowiedź nr 13.2:

500Mbps.

Pytanie nr 13.3:

3. Realizacja testów DDoS możliwa jest tylko w przypadku infrastruktury, która będzie dostępna z publicznej sieci Internet. Prosimy o potwierdzenie.

Odpowiedź nr 13.3:

Tak.

Pytanie nr 14.1:

Pytania odnośnie punktu 2.2.1.6. OPZ - Analiza i testy VPN oraz innych połączeń zdalnych:

1. Jaki rodzaj serwera VPN miałby podlegać testom (np.: IPSec, OpenVPN, WireGuard, Global Protect, inny)?

Odpowiedź nr 14.1:

IPsec.

Pytanie nr 14.2:

2. Ile serwerów (adresów IP) będzie podlegać weryfikacji?

Odpowiedź nr 14.2:

2.

Pytanie nr 14.3:

3. Czy prace mogą być realizowane w godzinach roboczych?

Odpowiedź nr 14.3:

Tak, po uzgodnieniu z Zamawiającym.

Pytanie nr 14.4:

4. Prosimy o informację czy audyt powinien zostać zrealizowany w modelu blackbox czy whitebox? Blackbox zakłada brak dodatkowej wiedzy o usłudze poza adresem IP, natomiast whitebox przewidujemożliwość przekazania Wykonawcy dostępów pozwalających zestawić tunel (np. login/hasło, plik konfiguracyjny, etc).

Odpowiedź nr 14.4:

Zamawiający podtrzymuje zapisy OPZ pkt 3.1.1.4. (testy blackbox/greybox).

Pytanie nr 15.1:

Pytania odnośnie punktu 2.2.1.7. OPZ - Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS):

1. Jakie rozwiązania IDS/IPS będą przedmiotem audytu (producent, wersja)?

Odpowiedź nr 15.1:

IDS / IPS będący częścią UTM'a.

Pytanie nr 15.2:

2. Prosimy o szerszy opis celu, jaki chcą Państwo osiągnąć przeprowadzając "Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS)"? Audyt ma skupić się na praktycznej weryfikacji konfiguracji systemów czy ma dotyczyć analizy konfiguracji oprogramowania?

Odpowiedź nr 15.2:

Wykonawca ma skupić się na praktycznej weryfikacji konfiguracji systemów IDS/IPS działających u Zamawiającego.

Pytanie nr 16.1:

Pytania odnośnie punktu 2.3.1.10. OPZ - Testy systemów kopii zapasowych i odzyskiwania danych:

Jaki system odpowiedzialny za proces wykonywania kopii zapasowych będzie przedmiotem audytu (producent, wersja)?

Odpowiedź nr 16.1:

Zamawiający korzysta z oprogramowania Veeam. Wersja oprogramowania zostanie podana po podpisaniu umowy z Zamawiającym.

Pytanie nr 16.2:

1. Prosimy o szerszy opis celu, jaki chcą Państwo osiągnąć przeprowadzając "Testy systemów kopii zapasowych i odzyskiwania danych."? Audyt ma skupić się na praktycznej weryfikacji konfiguracji systemów czy ma dotyczyć analizy konfiguracji oprogramowania?

Odpowiedź nr 16.2:

Wykonawca ma skupić się na praktycznej weryfikacji konfiguracji systemów.

Pytanie nr 17:

Pytania odnośnie punktu 2.2 OPZ - Infrastruktura sieciowa:

Ile podsieci występuje w całej sieci (pomiędzy iloma podsieciami należy zweryfikować poprawność segmentacji)?

Odpowiedź nr 17:

10.

Pytanie nr 18:

Czy Zamawiający mógłby rozważyć uznanie certyfikatu eWPT (Web Application Penetration Tester) za równoważny z certyfikatem CEH (Certified Ethical Hacker)?

Uzasadnienie:

1. Zakres umiejętności: Certyfikat eWPT, podobnie jak CEH, potwierdza szeroki wachlarz umiejętnościzwiązanych z przeprowadzaniem testów penetracyjnych aplikacji webowych. Osoby z certyfikatem eWPT posiadają zaawansowaną wiedzę w zakresie identyfikacji, analizy oraz eksploatacji luk w zabezpieczeniach aplikacji internetowych, co jest zgodne z zakresem kompetencjicertyfikatu CEH.
2. Renoma i uznanie: eWPT jest uznanym certyfikatem w środowisku pentesterskim, docenianym zarównoprzez pracodawców, jak i społeczność specjalistów w dziedzinie bezpieczeństwa IT. Wartość i skuteczność certyfikatu eWPT są potwierdzone przez liczne projekty, w których posiadacze tego certyfikatu z powodzeniem wdrażają swoje umiejętności.
3. Dostosowanie do standardów branżowych: eWPT, podobnie jak CEH, spełnia międzynarodowe standardyi najlepsze praktyki w zakresie cyberbezpieczeństwa, co w naszym przekonaniu czyni go odpowiednim w kontekście wymagań stawianych przez Zamawiającego.

Odpowiedź nr 18:

Zamawiający nie może uznać certyfikatu eWPT, ponieważ dotyczy on jedynie umiejętności tylko i wyłącznie z jednego obszaru, natomiast OZP obejmuje weryfikację wielu obszarów infrastruktury Zamawiającego, nie tylko aplikacji.

Pytania nr 19.a.-19.i.:

Pytanie nr 19.a.

Dotyczy wzór umowy §3
Czy Zamawiający wyrazi zgodę na zmianę zapisu na poniższy:

„Z uwagi na dynamikę postępu technicznego i spowodowane tym zmiany w sposobach uzyskiwania nieautoryzowanego dostępu do systemów informatycznych, Wykonawca nie gwarantuje, że po realizacji Umowy w zakresie, w jakim system informatyczny został przetestowany i wprowadzono zabezpieczenia rekomendowane w Raporcie, będzie on bezpieczny. Z powyższych względów Wykonawca nie ponosi odpowiedzialności za szkody Zamawiającego w przypadku nieautoryzowanej ingerencji w system informatyczny osób trzecich przy wykorzystaniu metod nieznanych w Momencie wykonywania Umowy przy uwzględnieniu aktualnego stanu wiedzy. W celu zwiększenia bezpieczeństwa systemów informatycznych Wykonawca zaleca periodyczne wykonywanie testów penetracyjnych. Wykonawca oświadcza, że w przypadku podłączenia do systemu informatycznego, będącego przedmiotem Umowy, prywatnych urządzeń osób trzecich, Wykonawca może uzyskać dostęp do tych urządzeń oraz do danych zapisanych na tych urządzeniach, co Zamawiający przyjmuje do wiadomości.

Zamawiający świadomy jest, że ryzykiem związanym z wykonywaniem elementów testów penetracyjnych jest możliwość całkowitej lub częściowej utraty danych

przechowywanych w systemie informatycznym będącym przedmiotem testów penetracyjnych, tym samym Zamawiający celem uniknięcia utraty danych powinien wykonać ich kopię zapasową i przechowywać ją w sposób uniemożliwiający ich utratę w toku wykonywania testów penetracyjnych. Zaniechanie w tym zakresie nie może obciążać Wykonawcy. Wykonawca nie odpowiada za całkowitą lub częściową utratę danych przechowywanych w systemie informatycznym będącym przedmiotem testów penetracyjnych.

Zamawiający świadomy jest, że ryzykiem związanym z wykonywaniem testów penetracyjnych jest możliwość całkowitej lub częściowej degradacji lub wyłączenia usług świadczonych za pośrednictwem systemu informatycznego będącego przedmiotem testów penetracyjnych. Wykonawca nie odpowiada za całkowitą lub częściową degradację lub wyłączenia usług świadczonych za pośrednictwem systemu informatycznego będącego przedmiotem testów penetracyjnych."

Pytanie nr 19.b.

Dotyczy wzór umowy §4 ust. 1

Prosimy o potwierdzenie czy określenie „nie później jednak niż w ciągu 14 dni kalendarzowych od dnia podpisania Umowy." odnosi się do terminu w jakim strony mogą uzgodnić inny termin przeprowadzenia testów czy też do terminu w jakim testy te powinny zostać przeprowadzone? Prosimy również o doprecyzowanie w jakiej formie mogą zostać dokonane uzgodnienia nowego terminu testów? Czy musi to być aneks czy też będzie wystarczająca inna forma?

Pytanie nr 19.c.

Dotyczy wzór umowy §4
Prosimy o dodanie poniższego zapisu :

„Wykonawca uprawniony jest do natychmiastowego zakończenia Testów penetracyjnych przed terminem, jeżeli w toku wykonywania Umowy okaże się, że system informatyczny będący przedmiotem testów penetracyjnych, wbrew, nie należy do Zamawiającego, lub też gdy w toku wykonywania testów penetracyjnych okaże się, że raport ma być wykorzystany w innym celu niż do ustalenia i poprawienia stanu bezpieczeństwa testowanego systemu informatycznego. W takim przypadku Zamawiający zobowiązany jest do uiszczenia pełnego wynagrodzenia Wykonawcy za czas pracy poświęcony na wykonanie Zamówienia do momentu zakończenia testów penetracyjnych z powyższej przyczyny, zaś raport z wykonania testów penetracyjnych nie zostanie przygotowany i Zamawiającemu nie przysługuje w tym zakresie jakiekolwiek roszczenie.".

Pytanie nr 19.d.

Dotyczy wzór umowy §8 pkt.1

Zawracamy się z prośbą o dodanie w pkt.1 zastrzeżenia, że odstąpienie może nastąpić po uprzednim wezwaniu Wykonawcę do rozpoczęcia realizacji Przedmiotu Umowy w dodatkowym terminie wskazanym w zwężaniu.

Pytanie nr 19.e.

Dotyczy wzór umowy §9 ust. 1 i ust. 2

W zakresie pkt. 1) zawracamy się z prośbą o wyjaśnienie jak procedura odbioru wpływa na prawo do naliczenia kary bo jest to niejasne. Zgodnie z umową Wykonawca po zakończeniu testów i sporządzeniu raportu powinien niezwłocznie, ale nie później niż w ciągu 3 dni roboczych od upływu terminu na realizację testów i sporządzenie raportu, zgłosić gotowość do odbioru. Natomiast protokół odbioru powinien zostać podpisany w ciągu kolejnych 3 dni roboczych. Ponadto zgodnie z umową dniem odbioru jest dzień podpisania protokołu odbioru. Wobec powyższego może zajść sytuacja, że gdy Wykonawca sporządzi raport w ostatnim dniu terminu przewidzianego w §4 ust. 2 odbiór prac zostanie dokonany dopiero 6 dni roboczych po upływie tego terminu na realizację przedmiotu umowy. Czy w takim przypadku Zamawiający będzie miał prawo naliczyć karę za zwłokę nawet jeżeli raport jest przygotowany zgodnie z wymaganą metodologią?

W zakresie pkt 2) prosimy o doprecyzowanie, czy kara za odstąpienie na podstawie §8 ust. 1 należy się tylko i wyłącznie w sytuacji gdy opóźnienie w rozpoczęciu realizacji przedmiotu umowy wynika z okoliczności zawinionych przez Wykonawcę. Wykonawca nie może być karany za opóźnienie jeżeli nie wynika ono z jego winy. Prosimy o zmianę treści na poniższą §9 ust. 2:

„W przypadku odstąpienia przez Zamawiającego od Umowy z przyczyn, o których mowa w § 8 ust. 1 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10 % maksymalnego wynagrodzenia brutto, o którym mowa w § 7 ust. 1 Umowy. Zdanie poprzedzające nie dotyczy przypadku opisanego w §8 ust. 1 pkt 1), gdy opóźnienie w rozpoczęciu realizacji przedmiotu umowy wynika z okoliczności niezawinionych przez Wykonawcę”

Pytanie nr 19.f.

Dotyczy wzór umowy §9 ust.3

Zgodnie z orzecznictwem w przypadku, gdy umowa przewiduje karę za odstąpienie, uprawniony w przypadku odstąpienia od umowy nie może żądać zapłaty innych kar umownych niż kara zastrzeżona za odstąpienie. Prosimy Zamawiającego o usunięcie tego postanowienia.

Pytanie nr 19.g.

Dotyczy wzór umowy §9 ust. 6

Prosimy o ograniczenie kary wyłącznie do informacji poufnych oraz u symetryzować tak by dotyczyła obydwu stron. W odniesieniu do danych osobowych ewentualna kara powinna zostać określona w umowie powierzenia danych osobowych do przetwarzania.

Pytanie nr 19.h.

Dotyczy wzór umowy §10
Prosimy o rozszerzenie zapisów w następujący sposób :

„1.Wykonawca przenosi na Zamawiającego, w ramach wynagrodzenia określonego w § 7 Umowy, majątkowe prawa autorskie do Raportu określonego w Umowie, z chwilą dokonania zapłaty ww. wynagrodzenia przez Zamawiającego, na następujących polach eksploatacji:

a) w zakresie utrwalania i zwielokrotniania Raportu, - wytwarzanie określoną techniką egzemplarzy raportu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową

b) w zakresie obrotu oryginałem albo egzemplarzami, na których Raport utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy

c) w zakresie rozpowszechniania Raportu w sposób inny niż określony w lit. b) - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym.

2.Wykonawca, w ramach wynagrodzenia określonego w Umowie, przenosi na Zamawiającego prawo do wykonywania zależnych praw autorskich do Raportu na polach eksploatacji określonych w ust. 1 powyżej.

3.Wykonawca, w ramach wynagrodzenia określonego w Umowie, przenosi na Zamawiającego własność egzemplarzy papierowych lub elektronicznych Raportu."

Pytanie nr 19.i.

Dotyczy wzór umowy
Zwracamy się z prośbą o dodanie poniższych zapisów:

„Zamawiający oświadcza, iż:

a) Wyraża zgodę na wykonanie przez Wykonawcę Testów penetracyjnych, których efektem może być uzyskanie przez Wykonawcę, w czasie wykonywania Testów penetracyjnych, nieautoryzowanego dostępu do systemu informatycznego Zamawiającego, w tym również do poszczególnych urządzeń połączonych z systemem informatycznym Zamawiającego. Wyrażenie zgody na uzyskanie dostępu do systemu informatycznego oraz poszczególnych urządzeń połączonych z tym systemem oznacza zgodę na uzyskanie dostępu przez Wykonawcę do danych przechowywanych w testowanym systemie informatycznym;

b) system informatyczny, będący przedmiotem Testów penetracyjnych, należy do Zamawiającego, a do systemu informatycznego nie powinny być podłączone żadne urządzenia niestanowiące własności Zamawiającego (w szczególności prywatne urządzenia osób fizycznych, np. pracowników Zamawiającego, współpracowników itp.) jak również na urządzeniach podłączonych do systemu informatycznego Zamawiającego nie powinny być przechowywane prywatne dane w/w osób;

c) w przypadku gdy elementem testowanego systemu informatycznego jest urządzenie lub usługa dostarczana przez osobę trzecią (np. serwer, rozwiązania „chmurowe" itp.) Zamawiający posiadać będzie zgodę takiej Strona 4 z 4 osoby trzeciej na wykonanie Testów penetracyjnych. Wszelkie oświadczenia osób trzecich o wyrażeniu powyższej zgody stanowić będą załącznik do Umowy;

d) świadomy jest, że podczas wykonywania Testów penetracyjnych istnieje możliwość uzyskania przez Wykonawcę tymczasowego dostępu do danych Zamawiającego, w tym danych poufnych stanowiących tajemnicę przedsiębiorstwa i/lub chronionych na podstawie odrębnych przepisów prawa, przechowywanych w systemie informatycznym będącym przedmiotem Testów penetracyjnych, na co wyraża zgodę;

e) świadomy jest, że ryzykiem związanym z wykonywaniem Testy penetracyjne jest możliwość całkowitej lub częściowej utraty danych przechowywanych w systemie informatycznym będącym przedmiotem Testów penetracyjnych, tym samym Zamawiający celem uniknięcia utraty danych powinien wykonać ich kopię zapasową i

przechowywać ją w sposób uniemożliwiający ich utratę w toku wykonywania Testów penetracyjnych – zaniechanie w tym zakresie nie może obciążać Wykonawcy;

f) świadomy jest, że ryzykiem związanym z wykonywaniem Testów penetracyjnych jest możliwość całkowitej lub częściowej degradacji lub wyłączenia usług świadczonych za pośrednictwem systemu informatycznego będącego przedmiotem Testów penetracyjnych;

g) w wyniku wykonywania Testów penetracyjnych (w tym również w wyniku sporządzenia i przekazania Raportu) nie zostanie zagrożone bezpieczeństwo Rzeczypospolitej Polskiej, jak również nie zostanie wyrządzona jakakolwiek szkoda Rzeczypospolitej Polskiej, a treść Raportu zostanie wykorzystana na potrzeby Zamawiającego.

h) jest świadomy, że z uwagi na dynamikę postępu technicznego i spowodowane tym zmiany w sposobach uzyskiwania nieautoryzowanego dostępu do systemów informatycznych, nie ma gwarancji, że po przeprowadzeniu Testów penetracyjnych w zakresie, w jakim system informatyczny został przetestowany, będzie on stale bezpieczny;

Zamawiający oświadcza, że system informatyczny będący przedmiotem Testów penetracyjnych w całości zlokalizowany jest na terenie siedziby Zamawiającego. Wykonawca uprawniony jest do zaprzestania wykonywania Testów penetracyjnych, jeżeli uzyska informację, iż system prawny kraju, na terenie którego zlokalizowany jest testowany system informatyczny, uniemożliwia przeprowadzenie Testów penetracyjnych w zakresie objętym niniejszą umową.

1. Zamawiający zobowiązany jest dostarczyć Wykonawcy wszelkie niezbędne dokumenty, w tym w szczególności umowy z dostawcami usług i dokumentacji oraz wykaz urządzeń podłączonych do testowanego systemu informatycznego niezbędnych do wykonania usług zawartych w umowie.

2. Strony zgodnie oświadcza, iż w przypadku uzyskania przez Wykonawcę dostępu do danych osobowych administrowanych przez Zamawiającego Strony zawrą odrębną umowę o powierzaniu przetwarzania danych osobowych.

3. Zamawiający zobowiązany jest do niezwłocznego przekazania Wykonawcy wszelkich informacji niezbędnych do prawidłowego wykonania przez Wykonawcę obowiązków określonych w niniejszej umowie,

a także do zapewnienia możliwości wykonania przedmiotu zlecenia w siedzibie podmiotu, którego system informatyczny stanowić będzie przedmiot usługi, jeżeli charakter Testów penetracyjnych będzie tego wymagał. Zobowiązanie to obejmuje w szczególności obowiązek udostępnienia na każde żądanie posiadanej infrastruktury informatycznej."

Odpowiedź nr 19.a. – 19.i.:

Zamawiający podtrzymuje zapisy PPU.

Pytanie nr 20:

Ile urządzeń, serwerów, jakie systemy operacyjne będą podlegały testom?

Odpowiedź nr 20:

100-150 serwerów, działających w oparciu o systemy Windows i Linux.

Pytanie nr 21:

Co oznacza i w jakim zakresie/czasie (liczba MD) ma być realizowane „Wsparcietechniczne w implementacji zaleceń wynikających z raportu końcowego dla wszystkich urządzeń oraz serwerów, bez naprawy błędów w aplikacjach dedykowanych.” W punkcie 3.1.4.3? Prosimy o wzięcie pod uwagę, że wykonawca nie zna środowiska zamawiającego ani jego konfiguracji, stąd nie ma pełnej wiedzy o możliwościach implementacji poprawek/zmian w środowisku zamawiającego oraz ichimplikacji na całe środowisko IT.

Odpowiedź nr 21:

Zgodnie z zapisami OPZ Zamawiający oczekuje realizacji wsparcia technicznego przez 60 dni Zamawiający nie potrafi oszacować niezbędnej pracochłonności w tym okresie, w szczególności gdy ta będzie uzależniona od wyników przedstawionych w raporcie i wskazanego w nim zakresu prac, który powinien być wykonany.

Pytanie nr 22:

Ile godzin należy zaplanować sesje QA oraz warsztaty o których mowa w pkt. 3.1.4.2? W zakresie warsztatów – jaki ma być ich zakres? Prosimy o wzięcie pod uwagę, że wykonawca nie zna środowiska zamawiającego ani jego konfiguracji, stąd nie ma pełnej wiedzy o możliwościach implementacji poprawek/zmian w środowisku zamawiającego oraz ich implikacji na całe środowisko IT.

Odpowiedź nr 22:

2 dni (16 godzin). Omówienie wyników raportów oraz rekomendacji w zakresie wprowadzenia zmian w systemach.

Pytanie nr 23:

Co oznacza, i jakich działań wymaga od wykonawcy punkt 3.1.1.10? „Przed rozpoczęciem prac audytowych niezbędne będzie wypełnienie stosownej deklaracji osób decyzyjnych zamawiającego oraz jednostki audytowanej świadczącej o zgodzie na działania i wiedzy nt. potencjalnych skutków działań testerów.”

Odpowiedź nr 23:

Zadanie to jest po stronie Zamawiającego. Zamawiający wskazał jedynie, że rozpoczęcie prac wymaga jego uprzedniej zgody.

Pytanie nr 24:

W jakim zakresie ma się odbyć „Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS)? Jakie dane udostępni Zamawiający w tym zakresie?

Odpowiedź nr 24:

Wykonawca ma skupić się na praktycznej weryfikacji konfiguracji systemów. Zamawiający po podpisaniu umowy udostępni Wykonawcy informację na temat wykorzystywanych przez siebie urządzeń.

Pytanie nr 25:

Czy wszystkie testy mogą być wykonane zdalnie?

Odpowiedź nr 25:

Tak, z wyłączeniem testów, które z uwagi na swoją specyfikę mogą wymagać obecności w siedzibie Zamawiającego.

Pytanie nr 26:

Jaki jest pożądany zakres testu w obrębie punktu „w zakresie podłączania obcych urządzeń" – czy chodzi o podłączenie komputera do sieci biurowej? Jeśli tak, w jakiej lokalizacji?

Odpowiedź nr 26:

Praktyczna weryfikacja pod kątem podłączenia obcego urządzenia do sieci Zamawiającego. Lokalizacja główna urzędu.

Pytanie nr 27:

Jakie są oczekiwania zakresu testów i jakie materiały przekaże zamawiający w zakresie realizacji punktu „Testy systemów kopii zapasowych i odzyskiwania danych."

Odpowiedź nr 27:

a) Testowanie tworzenia kopii zapasowych:
b) Testowanie procesu odzyskiwania danych.
d) Testowanie zgodności z politykami bezpieczeństwa i regulacjami:
Pozostałe niezbędne informacje Zamawiający przekaże po podpisaniu umowy.

Pytanie nr 28:

Jaki czas (w MD) wsparcia jest oczekiwany w punkcie „Czas na wsparcie odnośnie wdrażania rekomendowanych poprawek po wykonaniu testów i raportu to maksymalnie 60 dni kalendarzowych.

Odpowiedź nr 28:

Patrz odpowiedź na pytanie 21.

Pytanie nr 29:

Jaki jest wymagany zakres realizacji punktu „Sprawdzenie polityk zarządzania użytkownikami i kontrolą dostępu." – jaka jest objętość (liczba stron A4) polityk, które zamawiający przekaże do analizy w ramach tego punktu?

Odpowiedź nr 29:

Patrz odpowiedź na pytanie nr 6.

Pytanie nr 30:

Ile kont i w ilu oraz jakich systemach ma być przeanalizowanych w ramach punktu „Weryfikacja kont z dostępem administracyjnym i zakresu dostępów.”?

Odpowiedź nr 30:

Kilkanaście kont z uprawnieniami administracyjnymi. W 3 systemach (wirtualizacji, kopii zapasowych , kontroler domeny). Systemy zostaną wskazane po podpisaniu umowy.

Pytanie nr 31:

Ile baz i jakiego typu (producent, wersja) ma być przeanalizowanych w ramach punktu „Analiza i testy zabezpieczeń baz danych.”?

Odpowiedź nr 31:

2 bazy danych. Typy i wersja baz danych zostaną wskazane po podpisaniu umowy.

Pytanie nr 32:

Czy pożądane jest badanie konfiguracji, czy wyłącznie badania black/grey-box?

Odpowiedź nr 32:

Patrz odpowiedź na pytanie nr 1. Zamawiający oczekuje testów w modelach blackbox/ greybox lub innych czynności opisanych w OPZ lub wskazanych w odpowiedziach na inne pytania

Pytanie nr 33:

Krótki opis do czego służy aplikacja (np. aplikacja do realizacji transakcji bankowych, sklep internetowy) oraz kluczowe funkcje (lista głównych funkcji) oraz opis kategorii przetwarzanych danych (dane osobowe klientów, dane kartowe, dane transakcyjne, dane o stanie zdrowia etc.).

Pytanie nr 34:

Lista metod logowania/uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms), które mają zostać objęte testami.

Pytanie nr 35:

Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token (sprzętowy), kod sms, urządzenia HSM (HardwareSecurity Module, inne - proszę podać jakie), które mają zostać objęte testami.

Pytanie nr 36:

Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np.administrator – zarządza prawami dostępu innych użytkowników), które mają zostać objęte testami,

Pytanie nr 37:

Sumaryczna, orientacyjna liczba pól we wszystkich formularzach, które mają zostać objęte testami.

Pytanie nr 38:

Sumaryczna liczba parametrów wykorzystywanych w aplikacji które mają zostać objęte testami.

Odpowiedź nr 33 - 38:

Na pytania nr 33 – 38 Zamawiający udzieli niezbędnych informacji po podpisaniu Umowy z Wykonawcą. Założeniem Zamawiającego jest przeprowadzenie testów aplikacji webowych typu blackbox i greybox z zewnątrz przy bardzo ograniczonej wiedzy aspektów technicznych badanych aplikacji

Pytanie nr 39:

Do testów konfiguracji serwerów webowych z punktu 2.1.1.6 potrzebne będą uprawnienia administratora systemu operacyjnego na którym działa ten serwer WWW oraz dostęp na wszystkich portach TCP i UDP ze skanera przez sieć VPN OP. Czy taki dostęp będzie zapewniony?

Odpowiedź nr 39:

Odpowiedni dostęp zostanie udostępniony przez Zamawiającego.

Pytanie nr 40:

Krótki opis do czego służy aplikacja (np. aplikacja do realizacji transakcji bankowych, sklep internetowy) oraz kluczowe funkcje (lista głównych funkcji)oraz opis kategorii przetwarzanych danych (dane osobowe klientów, dane kartowe, dane transakcyjne, dane o stanie zdrowia etc.).

Pytanie nr 41:

Lista metod logowania/uwierzytelniania: (np. ID, hasło, certyfikat, token, kod sms), które mają zostać objęte testami.

Pytanie nr 42:

Lista metod autoryzacji operacji (jeśli występuje): (np. certyfikat, token (sprzętowy), kod sms, urządzenia HSM (HardwareSecurity Module, inne - proszę podać jakie), które mają zostać objęte testami.

Pytanie nr 43:

Liczba ról, które mają podlegać testom (np. gość, użytkownik zwykły, użytkownik rozszerzony, operator, administrator, itp.) wraz z krótkim opisem (np.administrator – zarządza prawami dostępu innych użytkowników), które mają zostać objęte testami.

Pytanie nr 44:

Sumaryczna, orientacyjna liczba pól we wszystkich formularzach, które mają zostać objęte testami.

Pytanie nr 45:

Sumaryczna liczba parametrów wykorzystywanych w aplikacji które mają zostać objęte testami.

Odpowiedź nr 40 - 45:

Na pytania nr 40 - 45 Zamawiający udzieli niezbędnych informacji po podpisaniu Umowy z Wykonawcą. Założeniem Zamawiającego jest przeprowadzenie testów aplikacji webowych typu blackbox i greybox z zewnątrz przy bardzo ograniczonej wiedzy o aspektów technicznych badanych aplikacji.

Pytanie nr 46:

Do testów konfiguracji serwerów webowych z punktu 2.1.1.6 potrzebne będą uprawnienia administratora systemu operacyjnego na którym działa ten serwerWWW oraz dostęp na wszystkich portach TCP i UDP ze skanera przez sieć VPN OP. Czy taki dostęp będzie zapewniony?

Odpowiedź nr 46:

Odpowiedni dostęp zostanie zapewniony przez Zamawiającego, przy czym Zamawiający ponownie wskazuje, że oczekuje testów aplikacji webowych z zewnątrz (aplikacje dostępne w sieci publicznej) pod kątem OWASP TOP10 oraz możliwości zidentyfikowania podatności, nie oczekuje weryfikacji konfiguracji od wewnątrz.

Pytanie nr 47:

Zakres adresacji IP objętych testami.

Odpowiedź nr 47:

Patrz odpowiedzi na poprzednie pytania nr 2 oraz 17.

Pytanie nr 48:

Orientacyjna liczba aktywnych IP w ramach adresacji objętej testami.

Odpowiedź nr 48:

Orientacyjnie liczba aktywnych IP w ramach adresacji objętej testami wynosi 600.

Pytanie nr 49:

Proszę podać godziny, w których można przeprowadzać testy, oraz dni i godziny, w których środowiska testowe będą dostępne.

Odpowiedź nr 49:

Zamawiający planuje przeprowadzenie testów na środowiskach produkcyjnych w dowolnych godzinach zgodnie z pkt 3.1.1.7. po uzgodnieniu harmonogramu z Zamawiającym z uwzględnieniem zapisów w pkt. 3.1.1.6.

Pytanie nr 50:

Prosimy o specyfikację komponentów infrastruktury, które mają być objęte testami.

50.a. Rodzaj (np. serwer aplikacyjny, serwer www, serwer bazodanowy, system operacyjny Windows, system operacyjny Linux, drukarka, skaner, urządzenie aktywne, inne, itp.).

50.b. Producent.

50.c. Wersja.

50.d. Dla baz danych prosimy o podanie liczby baz danych dla każdej z instancji z baz danych, które mają być objęte testami.

Odpowiedź nr 50.a. – 50.d:

Zamawiający podtrzymuje zapisy OPZ pkt 3.1.1.4. Odp. Zostały udzielone w pkt. 14.2, 14.4. oraz 31.

Pytanie nr 51:

Do testów konfiguracji potrzebne będą uprawnienia administratora do każdego badanego komponentu infrastruktury czy też urządzenia. oraz dostęp na wszystkich portach TCP i UDP ze skanera przez sieć VPN OP. Czy taki dostęp będzie zapewniony?

Odpowiedź nr 51:

Patrz odpowiedź w pkt 7 - Odpowiedni dostęp zostanie udzielony przez Zamawiającego. Zamawiający dopuszcza instalację w sieci wewnętrznej urządzenia Wykonawcy, przy czym dostęp do takiego urządzenia z zewnątrz będzie wymagał dostępu z wykorzystaniem VPN Zamawiającego.

Pytanie nr 52:

IP adresy, które będą podlegały audytowi:
Lista/szacunkowa liczba aktywnych IP adresów świadczących usługi.

Odpowiedź nr 52:

Odp. W pkt 2. Orientacyjnie liczba aktywnych IP w ramach adresacji objętej testami wynosi 600.

Pytanie nr 53:

Prosimy o listę i liczbę urządzeń sieciowych do realizacji punktu 2.2.1.4

Odpowiedź nr 53:

Zamawiający informuje że, posiada 82 urządzenia.

Pytanie nr 54:

Prosimy o listę i liczbę połączeń zdalnych oraz rodzaj używanego VPN do realizacji punktu 2.2.1.6

Odpowiedź nr 54:

Zmawiający informuje, że używa IPsec.

Pytanie nr 55:

Prosimy o listę i liczbę urządzeń IPS/IDS do realizacji punktu 2.2.1.7.

Odpowiedź nr 55:

Zamawiający informuje, że posiada 2 urządzenia.

Pytanie nr 56:

Czy będzie możliwy dostęp na wszystkich portach TCP i UDP przez VPN OP do całej sieci serwerowej i infrastruktury sieciowej ze stacji pentestera do realizacji całego punktu 2.2 i 2.3 ? Jeśli nie to czy realizacja tego punktu będzie możliwa zdalnie poprzez umieszczenie w sieci serwerowej klienta urządzenia OP podłączonego do internetu ?

Odpowiedź nr 56:

Patrz odpowiedź na pytanie nr 39.

Pytanie nr 57:

Czy klient oczekuje w punkcie 2.3.1.10 testów bezpieczeństwa systemu backupowego (test techniczny) , czy raczej sprawdzenia poprawności procedur tworzenia i odzyskiwania kopii zapasowych (audyt proceduralny) ?

Odpowiedź nr 57:

Wykonawca powinien skupić się na praktycznej weryfikacji konfiguracji systemów (test techniczny).

Pytanie nr 58:

Ile scenariuszy ataku phishingowego ma zostać przygotowane (punkt 2.4.1.2)

Odpowiedź nr 58:

Zamawiający informuje że, oczekuje 2 scenariuszy.

Pytanie nr 59:

Ilu pracowników ma być objętych testami?

Odpowiedź nr 59:

Zgodnie z pkt. OPZ 2.4.1.4. – 100.

Pytanie nr 60.a.-60.c.:

Jakie typy ataków mają być testowane? Przykładowo: udp flood, icmp flood,

Odpowiedź nr 60.a.:

Zamawiający nie przewiduje określania szczegółowych informacji w tym zakresie.

Pytanie nr 60.b:

Ataki na protokoły (syn flood itp., fragment packet attack,).

Odpowiedź nr 60.b.:

Zamawiający nie przewiduje określania szczegółowych informacji w tym zakresie.

Pytanie nr 60.c:

Ataki na L7.

Odpowiedź nr 60.c.:

Zamawiający nie przewiduje określania szczegółowych informacji w tym zakresie.

Pytanie nr 61:

Jaki wolumen ruchu powinien być wg. Państwa wykorzystany do testów?:

Odpowiedź nr 61:

Zamawiający informuje, że wolumen ataku powinien wynosić nie mniej niż 500 Mpbs.

Pytanie nr 62.a. – 62.b.:

Jakie mają być parametry symulacji ataku DDoS na wskazany przez Zamawiającego adres:

a. jaki poziom ruchu (pps/bps/rps)

Odpowiedź nr 62.a.:

Patrz odpowiedź na pytanie 61.

b. która warstwa (sieciowa, szyfrowanego tunelu, http, procesy biznesowe, cache/lb)

Odpowiedź nr 62.a. 62.b.:

Zamawiający nie przewiduje określania szczegółowych informacji odnośnie typów ataku DDoS.

Pytanie nr 63:

Czy są ograniczenia odnośnie źródeł z jakich pochodzi ruch podczas symulacji ataku miałby pochodzić?

Odpowiedź nr 63:

Zamawiający informuje, że nie ma ograniczeń odnośnie symulacji ataku.

Pytanie nr 64:

Czy zostały zdefiniowane usługi, które zostaną poddane testom? (sugerowane min.: smtp, dns, http/s)

Odpowiedź nr 64:

Zamawiający informuje, że testowane usługą są uzależnione od wymagań OPZ (m.in. są to aplikacje webowe, VPN, IDS/IPS czy inne określone w OPZ.

Pytanie nr 65:

Czy przed testami ma być przeprowadzony przegląd architektury wewnętrznej sieci lub seminarium w celu lepszego zaprojektowania testów?

Odpowiedź nr 65:

Zamawiający nie przewiduje przeglądu architektury lub seminarium.

Pytanie nr 66:

Czy w czasie testów będą wyłączone mechanizmy bezpieczeństwa np. antyspam, antyDDoS, firewalle?

Odpowiedź nr 66:

Zamawiający nie przewiduje wyłączania jakichkolwiek mechanizmów bezpieczeństwa. Celem testów jest weryfikacje tych mechanizmów w środowiskach Zamawiającego, więc ich wyłączenie byłoby niecelowe.

Pytanie nr 67:

Szacowana liczba kont w poszczególnych domenach. Jeśli to możliwe - z podziałem na typy tych kont.

Odpowiedź nr 67:

Zamawiający odsyła m.in. do odpowiedzi na pytanie 30.

Pytanie nr 68:

Liczba systemów w ramach domeny. Jeśli to możliwe - z podziałem na typy oraz wersje systemów operacyjnych.

Odpowiedź nr 68:

Zamawiający nie przewiduje podawania tak szczegółowych informacji. Informacje dotyczące testowanej infrastruktury zostały wskazane w OPZ oraz odpowiedziach na inne pytania. Informacje niepubliczne dotyczące infrastruktury, jeżeli będą niezbędne do wykonania testów, zostaną udzielone po podpisaniu umowy.

Pytanie nr 69:

Liczba i opis wykorzystywanych komponentów dodatkowych (np. DNS).

Odpowiedź nr 69:

Zamawiający nie przewiduje podawania tak szczegółowych informacji. Informacje dotyczące testowanej infrastruktury zostały wskazane w OPZ oraz odpowiedziach na inne pytania. Informacje niepubliczne dotyczące infrastruktury, jeżeli będą niezbędne do wykonania testów, zostaną udzielone po podpisaniu umowy.

Pytanie nr 70:

Liczba oraz opis dodatkowych interfejsów wykorzystywanych w ramach AD (połączenia cloud-onprem, delegacje, systemy zarządzania konfiguracją, integracje z innymi systemami zarządzania tożsamością lub systemami PAM, ADFS, połączenia z aplikacjami).

Odpowiedź nr 70:

Zamawiający nie przewiduje podawania tak szczegółowych informacji. Informacje dotyczące testowanej infrastruktury zostały wskazane w OPZ oraz odpowiedziach na inne pytania. Informacje niepubliczne dotyczące infrastruktury, jeżeli będą niezbędne do wykonania testów, zostaną udzielone po podpisaniu umowy.

Pytanie nr 71:

Liczba użytkowników w domenie.

Odpowiedź nr 71:

Zamawiający informuje, że przybliżona liczba to 1200.

Pytanie nr 72:

Liczba domen z jakich składa się las.

Odpowiedź nr 72:

Zamawiający nie przewiduje podawania tak szczegółowych informacji. Informacje dotyczące testowanej infrastruktury zostały wskazane w OPZ oraz odpowiedziach na inne pytania. Informacje niepubliczne dotyczące infrastruktury, jeżeli będą niezbędne do wykonania testów, zostaną udzielone po podpisaniu umowy.

Pytanie nr 73:

Czy Zamawiający dopuszcza modyfikację zapisu §4 ust.1 tak by termin rozpoczęcia testów penetracyjnych liczony będzie od przekazania działających dostępów?

Jeśli NIE, to: - jaki jest deklarowany czas przekazania w/w dostępów?

Odpowiedź nr 73:

Termin rozpoczęcia testów penetracyjnych liczony będzie od przekazania dostępów Wykonawcy przez Zamawiającego.

Pytanie nr 74:

2.2.1.7. Testy systemów wykrywania i zapobiegania włamaniom (IDS/IPS)

- Czy zamawiający ma na myśli testy bezpieczeństwa samych systemów, czy ich skuteczności w wykrywaniu ataków?

- Jeśli testy skuteczności to czy zostanie zapewniona asysta Zamawiającego lub dostęp do w/w systemów?

Odpowiedź nr 74:

Zamawiający ma na myśli weryfikację skuteczności funkcjonujących u niego zabezpieczeń podczas ataków na infrastrukturę. Tak, asysta będzie zapewniona w niezbędnym zakresie.

Pytanie nr 75:

2.3.1.10. Testy systemów kopii zapasowych i odzyskiwania danych

- Czy zamawiający ma na myśli przeprowadzenie testów bezpieczeństwa tych systemów, czy testów odtworzeniowych

Odpowiedź nr 75:

Zamawiający ma na myśli prowadzenie testów odtworzeniowych wybranego serwera..

Pytanie nr 76:

Ile aplikacji będzie testowane?

Odpowiedź nr 76:

2.

Pytanie nr 77:

Do czego służą aplikacje?

Odpowiedź nr 77:

Odpowiedź w pytaniach nr 33-38.

Pytanie nr 78:

Jakie są kluczowe (krytyczne) funkcjonalności aplikacji?

Odpowiedź nr 78:

Odpowiedź w pytaniach nr 33-38.

Pytanie nr 79:

Rodzaj testów bezpieczeństwa: black box, white box, grey box?

Odpowiedź nr 79:

Zamawiający podtrzymuje zapisy OPZ pkt 3.1.1.4. (testy blackbox/greybox).

Pytanie nr 80:

Czy aplikacja przechodziła już testy bezpieczeństwa?

Odpowiedź nr 80:

Tak.

Pytanie nr 81:

Rodzaj środowiska: testowe/produkcja?

Odpowiedź nr 81:

Produkcja.

Pytanie nr 82:

Czy aplikacja zawiera dane klientów, osobowe, dane finansowe lub inne dane wrażliwe?

Odpowiedź nr 82:

Tak.

Pytanie nr 83:

Czy jest możliwość prowadzenia testów zdalnie?

Odpowiedź nr 83:

Patrz odpowiedź na pytanie nr 25.

Pytanie nr 84:

Czy aplikacja wykorzystuje API? Jeżeli tak to jakie (REST, SOAP, inne)?

Odpowiedź nr 84:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 85:

Jaka jest szacunkowa ilość podstron aplikacji oraz metod API (100, 1 000, 10 000)?

Odpowiedź nr 51:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 86:

Jaka jest szacunkowa ilość formularzy? Jako formularz należy przyjąć podstronę na której użytkownik wprowadza dane np. panel logowania, formularz kontaktowy, składanie wniosków itp.

Odpowiedź nr 86:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 87:

Jaka jest lista metod logowania i uwierzytelniania: ID, hasło, token, mail, sms itp.?

Odpowiedź nr 87:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 88:

Czy istnieją dodatkowe metody autoryzacji operacji wykonywanych w aplikacji? sms, email, klucz zewnętrzny?

Odpowiedź nr 88:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 89:

Czy aplikacja jest zlokalizowana na serwerach własnych klienta czy u dostawcy zewnętrznego?

Odpowiedź nr 89:

Patrz odpowiedzi udzielonych na pytania nr 33 – 38.

Pytanie nr 90:

Czy aplikacja jest chroniona przez firewall? sieciowy/aplikacyjny/inny? Jeżeli tak, czy będzie on aktywny podczas testów?

Odpowiedź nr 90:

Patrz odpowiedź na pytanie nr 66.

Pytanie nr 91:

Jaka jest liczba ról, grup, uprawnień używanych przez aplikację? np. użytkownik, manager, administrator?

Odpowiedź nr 91:

Patrz odpowiedź na pytanie nr 33- 38 oraz 40 – 45.

Pytanie nr 92.a. – 92.i.:

Dodatkowo dla testów whitebox:

a. W jakim języku programowania napisana jest aplikacja?

Odpowiedź nr 92.a.:

Zamawiający nie przewiduje testów whitebox.

b. Ile MB/KB zajmuje aplikacja?

Odpowiedź nr 92.b.:

Patrz odpowiedź na pytanie nr 33- 38.

c. Szacunkowa Ilość linijek kodu?

Odpowiedź nr 92.c.:

Patrz odpowiedź na pytanie nr 33- 38.

d. Szacunkowa ilość klas?

Odpowiedź nr 92.d.:

Patrz odpowiedź na pytanie nr 33- 38

e. Jakie są dodatkowe wtyczki lub technologie używane przez aplikację?

Odpowiedź nr 92.e.:

Patrz odpowiedź na pytanie nr 33- 38 oraz 40 – 45.

f. Czy na systemie można wykonywać ataki niebezpieczne np. atak który wyłączy maszynę aplikacyjną?

Odpowiedź nr 92.f.:

Tak, po uzgodnieniu z Zamawiającym.

g. Czy aplikacja obejmuje testy konfiguracji?

Odpowiedź nr 92.g.:

Patrz odpowiedź na pytanie nr 1 oraz 3.

h. Czy aplikacja chroniona jest przez firewall?

Odpowiedź nr 92.h.:

Patrz odpowiedź na pytanie nr 66.

i. Czy jest dostępna dokumentacja aplikacji?

Odpowiedź nr 92.i.:

Patrz odpowiedź na pytanie nr 33- 38 oraz 40 – 45.

Zamawiający wprowadza następujące zmiany do Zaproszenia:

Miejsce, w którym znajduje się zmieniany tekst	***Zamiast:***	***Powinno być:***
Termin złożenia oferty str. 4 Zaproszenie	Oferty należy składać mailowo w terminie do dnia **19 września 2024 r.** do godz. **10:00**	Oferty należy składać mailowo w terminie do dnia **24 września 2024 r.** do godz. **16:00**