Numer sprawy: **Izp.271.33.2024 Załącznik numer 6a do SWZ**

**Zadanie nr 1**

Spis treści

[1 AUDYT SZBI ORAZ AKTUALIZACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W TYM POLITYKI BEZPIECZEŃSTWA INFORMACJI. 2](#_Toc177421884)

[2 TESTY PENETRACYJNE INFRASTRUKTURY INFORMATYCZNEJ 5](#_Toc177421885)

[3 SZKOLENIE BUDUJĄCE ŚWIADOMOŚĆ CYBERZAGROŻEŃ I SPOSOBÓW OCHRONY DLA PRACOWNIKÓW URZĘDU W FORMIE DOSTĘPU DO PLATFORMY SZKOLENIOWEJ 11](#_Toc177421886)

[4 SZKOLENIA Z TESTAMI SOCJOTECHNICZNYMI DLA PRACOWNIKÓW URZĘDU 15](#_Toc177421887)

[5 SZKOLENIA SPECJALISTYCZNE DLA KADRY ZARZĄDZAJĄCEJ URZĘDU Z ZAKRESU CYBERBEZPIECZEŃSTWA 20](#_Toc177421888)

f

## 1 AUDYT SZBI ORAZ AKTUALIZACJA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI W TYM POLITYKI BEZPIECZEŃSTWA INFORMACJI.

|  |  |  |
| --- | --- | --- |
| L.P | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Zamówienie będzie realizowane na rzecz **Urzędu Miasta Bielsk Podlaski.** | SPEŁNIA TAK /NIE |
|  | Wykonawca jest zobowiązany do przeprowadzenia w poszczególnych latach realizacji projektu pn. „Cyberbezpieczny Samorząd” współfinansowanego w ramach środków Unii Europejskiej i budżetu państwa w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytetu II Zaawansowane usługi cyfrowe, Działania 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa , tj. w roku 2024, 2025 audytu systemu zarządzania bezpieczeństwem informacji w związku z zapisami w § 19 ust. 2 pkt 14 Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2024 poz. 773), zwanego dalej „audytem KRI” dla Zamawiającego. | SPEŁNIA TAK /NIE |
|  | Wykonawca jest zobowiązany do przeprowadzenia aktualizacji i wdrożenia kompletnego Systemu Zarządzania Bezpieczeństwem Informacji (dalej zwany: SZBI) dla Zamawiającego. | SPEŁNIA TAK /NIE |
|  | Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność  z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI oraz zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2023 dla Zamawiającego. | SPEŁNIA TAK /NIE |
|  | Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczony do Zamawiającego w formie elektronicznej. | SPEŁNIA TAK /NIE |
|  | Audyt KRI oraz aktualizacja i wdrożenie SZBI dla Zamawiającego muszą zostać przeprowadzone przez:  1) audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz. U. 2018 poz. 1999) lub; | SPEŁNIA TAK /NIE |
|  | 2) audytora wewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U. 2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001:2023. | SPEŁNIA TAK /NIE |
|  | Wykonawca w trakcie realizacji zamówienia jest zobowiązany do zapoznania się  z częściowo wypełnioną ankietą dojrzałości cyberbezpieczeństwa w zakresie wskazanym przez Zamawiającego oraz uwzględnić w ramach aktualizacji i wdrożenia SZBI planowany w ramach realizacji projektu zakres usprawnień SZBI. | SPEŁNIA TAK /NIE |
|  | Wykonawca po wykonaniu ostatniego audytu KRI jest zobowiązany do uzupełnienia ankiety dojrzałości cyberbezpieczeństwa. Ankietę dojrzałości cyberbezpieczeństwa należy wypełnić w oparciu o aktualny na dzień wypełnienia ankiety wzór ankiety opublikowany na stronie: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad (załącznik nr 6 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych). | SPEŁNIA TAK /NIE |
|  | Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta” dla Zamawiającego na podstawie zebranych przez Wykonawcę danych. Zamawiający nie dopuszcza pozostawienia pustych pól dla określonych powyżej kolumn, w przypadku jeżeli w polu opisowym nie przewiduje się zmian wówczas należy zamieścić odpowiednią informację. Ankieta dojrzałości cyberbezpieczeństwa zostanie podpisana przez audytora dokonującego audyt KRI przy wykorzystaniu kwalifikowalnego podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej. | SPEŁNIA TAK /NIE |
|  | Wykonawca przy świadczeniu usług jest zobowiązany uwzględnić i zastosować wymagania Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) oraz akty wykonawcze wydane do niej. W przypadku jeżeli w okresie realizacji zamówienia zostanie przyjęta ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw bądź inne przepisy implementujące Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) w polski system prawny Wykonawca ma obowiązek uwzględnić wszystkie ich wymagania przy świadczeniu usług objętych niniejszym zamówieniem zarówno w trakcie realizacji zamówienia jak i w trakcie okresu gwarancji. | SPEŁNIA TAK /NIE |
|  | Na wszystkie usługi Wykonawca udzieli 12-miesięcznej gwarancji jednak nie dłużej niż do dnia miesiąca czerwca 2026 r. polegającej na wprowadzaniu niezbędnych zmian w dokumentacji i aktualizacji dokumentacji na podstawie stwierdzonych przez Zamawiającego niezgodności dokumentacji z bieżącym stanem w okresie gwarancji. | SPEŁNIA TAK /NIE |
|  | Zamawiający informuje, że tam, gdzie Zamawiający opisał przedmiot zamówienia przez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza się rozwiązania równoważne opisywanym. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia. | SPEŁNIA TAK /NIE |
|  | Zamawiający informuje, że tam, gdzie w opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne , pod warunkiem, że będą one o nie gorszych właściwościach i jakości. Zamawiający informuje, iż w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy jakie cechy powinny posiadać materiały użyte do realizacji przedmiotu zamówienia. Ewentualne użycie nazwy producenta ma wyłącznie charakter przykładowy i ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. | SPEŁNIA TAK /NIE |
|  | Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego złożenia stosownych dokumentów, uwiarygodniających te rozwiązania. | SPEŁNIA TAK /NIE |
|  | Wykonawca, który posługuje się równoważnymi certyfikatami lub normami musi je załączyć do oferty. Przez certyfikat lub normę równoważną Zamawiający rozumie certyfikat lub normę analogiczną co do zakresu z certyfikatami lub normami wskazanymi z nazwy, który potwierdza spełnianie certyfikacji lub normy charakteryzującej się cechami właściwymi dla certyfikacji lub normy wymienionej przez Zamawiającego, wystawiony przez niezależny podmiot uprawniony do certyfikacji. | SPEŁNIA TAK /NIE |

## 2 TESTY PENETRACYJNE INFRASTRUKTURY INFORMATYCZNEJ

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne) Oferowane parametry** | **Oferowane parametry** |
|  | Informacje ogólne | * Głównym celem testów bezpieczeństwa jest identyfikacja możliwie wielu luk w zabezpieczeniach aplikacji, w szczególności tych, które mogą mieć poważny wpływ na atrybuty bezpieczeństwa systemów i danych przetwarzanych przez systemy (poufność, integralność, dostępność). * Testowanie bezpieczeństwa aplikacji internetowych ma symulować działania typowych aktorów zagrożeń, które zazwyczaj należą do jednej z dwóch grup:   + Użytkownik anonimowy – użytkownik, który nie posiada poświadczeń pozwalających na uwierzytelnienie w aplikacji docelowej.   + Użytkownik uwierzytelniony – użytkownik, który posiada poświadczenia pozwalające na uwierzytelnienie w aplikacji docelowej. * Prace zostaną przeprowadzone zdalnie z wykorzystaniem połączenia VPN do zasobów Zamawiającego. * Prace będą wykonywane z jednego stałego adresu IP Wykonawcy. * Testy bezpieczeństwa muszą objąć wymagania weryfikacyjne określone w następujących dokumentach:   + OWASP Web Security Testing Guide v4.2,   + OWASP Top 10 2021,   + OWASP Application Security Verification Standard (ASVS) v4.0.3 (Level 2),   Przebieg procesu testowania bezpieczeństwa aplikacji | SPEŁNIA TAK /NIE |
|  | Przebieg procesu testowania bezpieczeństwa aplikacji: | * Identyfikacja wersji wykorzystywanego oprogramowania, * Przegląd repozytoriów podatności w celu weryfikacji istnienia podatności dla zidentyfikowanych wersji oprogramowania, * Przegląd źródeł prezentowanych stron serwisu internetowego w celu identyfikacji potencjalnych luk w bezpieczeństwie, * Uzyskanie dodatkowych informacji z wykorzystaniem technik google hacking, * Przegląd funkcji oraz zabezpieczeń aplikacji, w tym m.in.: weryfikacja poziomu zabezpieczenia sesji klientów aplikacji (TLS), analiza metod uwierzytelniania użytkowników, identyfikacja metod walidacji danych wejściowych, * Przegląd aplikacji w celu: identyfikacji architektury i logiki aplikacji (tzw. „spidering”), wstępnej weryfikacji metod walidacji danych wejściowych, analizy metod zarządzania sesjami użytkowników, * Analiza logiki aplikacji (z punktu widzenia ryzyka utraty integralności, poufności * i dostępności przetwarzanych danych oraz rozliczalności działań użytkowników, a także określenie możliwych do wykonania operacji oraz ich istotności dla funkcjonowania procesów biznesowych) * Testowanie efektywności walidacji wprowadzanych danych i kodowania danych wyjściowych (m.in. próby ataków „Cross Site Scripting”, „SQL Injection”, „LDAP Injection”, „XML Injection”, „XPATH Injection”, próby „directory traversal”, próby wywołania poleceń systemowych, próby przepełnienia bufora pamięci) * Analiza mechanizmów zarządzania sesjami użytkowników (m.in. identyfikacja schematu zarządzania sesją, weryfikacja sposobu przekazywania identyfikatorów sesji, manipulacja identyfikatorami sesji, analiza metod ochrony identyfikatorów sesji, weryfikacja konfiguracji czasu trwania sesji, weryfikacja odporności na ataki przejęcia sesji, weryfikacja dodatkowych mechanizmów ochronnych broniących przed atakami takimi jak „Cross-site Request Forgery”) * Weryfikacja mechanizmów uwierzytelniających (m.in. stosowanie domyślnych, łatwych do odgadnięcia haseł, próby siłowego/słownikowego łamania haseł, próby obejścia schematu uwierzytelniania, analiza bezpieczeństwa funkcji przypomnienia/resetu haseł, weryfikacja efektywności funkcji wylogowania z aplikacji) * Analiza mechanizmów kontroli dostępu (m.in. identyfikacja modelu kontroli dostępu, analiza skuteczności kontroli dostępu poprzez próby pionowej i poziomej eskalacji uprawnień tj. bezpośredni dostęp do obiektów, funkcji i adresów URL, próby listowania zawartości katalogów, weryfikację czy odpowiedzi serwera nie zawierają nadmiarowych danych) * Weryfikacja mechanizmów przetwarzania i przechowywania danych (m.in. analiza działania mechanizmów pamięci podręcznej przeglądarki oraz serwerów pośredniczących, weryfikacja mechanizmów ochrony lokalnie zapisywanych danych, analiza metod przekazywania danych pomiędzy aplikacją i serwerem oraz komponentami aplikacji takimi jak np. aplet Java) * Analiza rozwiązań kryptograficznych (m.in. weryfikacja poprawności implementacji rozwiązań kryptograficznych) * Ataki typu odmowa usługi (m.in. analiza możliwości blokowania kont innych użytkowników, próby przepełnienia bufora pamięci, próby przekroczenia limitów zasobów dostępnych dla użytkowników serwisu) * Analiza mechanizmów obsługi błędów (m.in. weryfikacja czy komunikaty błędów nie ujawniają nadmiarowych informacji, weryfikacja czy wystąpienie błędu nie pozwala na eskalację uprawnień, próby manipulacji komunikatami błędów) * Weryfikacja konfiguracji protokołu HTTP * (m.in. analiza stosowanych metod HTTP, analiza obecności nagłówków regulujących pracę mechanizmów powiązanych z bezpieczeństwem np. zapobieganie atakom Clickjacking, automatycznemu wykrywaniu treści, analiza implementacji HSTS, CSP, CORS) * Analiza implementacji protokołów SSL/TLS (ocena stosowanych zestawów szyfrów, analiza konfiguracji parametrów połączeń SSL/TLS, weryfikacja stosowanych certyfikatów, identyfikacja dodatkowych mechanizmów zabezpieczeń takich jak HTTP Strict Transport Security oraz HTTP Public Key Pinning)   Testy bezpieczeństwa aplikacji muszą wykorzystywać automatyczne narzędzia służące do weryfikacji poziomu bezpieczeństwa aplikacji internetowych i infrastruktury oraz przy wykorzystaniu technik manualnych.  Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów:   * Burp Suite Pro * DirBuster * Nikto * Nessus Professional * FOCA * Testssl * Narzędzia i autorskie skrypty w Kali Linux | SPEŁNIA TAK /NIE |
|  | Wykaz aplikacji, które podlegają testom: | * Portal Mieszkańca (producent ZETO Białystok) - testy części aplikacji mieszkańców, oraz pracowników po zalogowaniu się; * Portal Obsługi Mieszkańca - testy bezpieczeństwa aplikacji wewnętrznej dla pracowników; * System informacji przestrzennej - testy części aplikacji mieszkańców, oraz pracowników po zalogowaniu się; * Portal e-usług geodezyjnych - testy części aplikacji mieszkańców; * Testy bezpieczeństwa aplikacji:   + Drogi, GemaOnline, Mienie, MPZP, SIP, Wuetka, Manager do których pracownicy logują się loginem i hasłem. | SPEŁNIA TAK /NIE |
|  | Zewnętrzne testy penetracyjne infrastruktury informatycznej | * Próby zgromadzenia jak największej ilości dostępnych publicznie informacji na temat infrastruktury informatycznej * Identyfikacja zakresu adresów IP * Identyfikacja udostępnionych usług poprzez skanowanie portów TCP/UDP wraz z próbą uzyskania informacji o zainstalowanych wersjach oprogramowania wykorzystując techniki fingerprinting oraz banner grabbing * Uzyskanie publicznie dostępnych informacji o organizacji i jej infrastrukturze np. poprzez wykorzystanie technik google hacking, DNS zone transfer, czy w przypadku sieci wewnętrznej prowadząc nasłuch ruchu w sieci * Skanowanie podatności z wykorzystaniem automatycznych narzędzi, * Manualna identyfikacja podatności w oparciu o zgromadzone informacje o wersjach zainstalowanego na badanych urządzeniach oprogramowania w publicznych bazach (np. Bugtraq, CERT, OSVDB), * Analiza mająca na celu weryfikację i eliminację potencjalnych fałszywych alarmów (false positives) oraz identyfikację krytycznych podatności, * Próba odnalezienia kodu oprogramowania wykorzystującego daną podatność – tzw. exploit * Kontrolowane próby wykorzystania stwierdzonych podatności   Testy penetracyjne realizowane będą w oparciu o globalną metodykę, zgodną z opracowaniami OSSTMM (Open Source Security Testing Methodology Manual) LPT (License Penetration Testing) oraz najlepszymi praktykami w obszarze testów penetracyjnych   * Testy penetracyjne infrastruktury prowadzone będą z wykorzystaniem automatycznych narzędzi służących do weryfikacji poziomu bezpieczeństwa infrastruktury oraz przy wykorzystaniu technik manualnych, * Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów zewnętrznych:   + Nmap   + Nessus Professional   + OpenVAS   + MetaSploit   + Kain & Abel   + Wireshark   + Maltego   + RainbowCrack   + Foca | SPEŁNIA TAK /NIE |
|  | Testy penetracyjne infrastruktury wewnętrznej | * Próby zgromadzenia jak największej ilości dostępnych publicznie informacji na temat infrastruktury informatycznej * Identyfikacja udostępnionych usług poprzez skanowanie portów TCP/UDP wraz z próbą uzyskania informacji  o zainstalowanych wersjach oprogramowania wykorzystując techniki fingerprinting oraz banner grabbing * Skanowanie podatności z wykorzystaniem automatycznych narzędzi * Manualna identyfikacja podatności * w oparciu o zgromadzone informacje * o wersjach zainstalowanego na badanych urządzeniach oprogramowania w publicznych bazach (np. Bugtraq, CERT, OSVDB), * Analiza mająca na celu weryfikację i eliminację potencjalnych fałszywych alarmów (false positives) oraz identyfikację krytycznych podatności, * Próba odnalezienia kodu oprogramowania wykorzystującego daną podatność – tzw. exploit * Kontrolowane próby wykorzystania stwierdzonych podatności   Testy podatności są realizowane w oparciu o globalną metodykę, zgodną z opracowaniami OSSTMM (Open Source Security Testing Methodology Manual) LPT (License Penetration Testing) oraz najlepszymi praktykami w obszarze testów podatności.   * Testy penetracyjne infrastruktury prowadzone będą z wykorzystaniem automatycznych narzędzi służących do weryfikacji poziomu bezpieczeństwa infrastruktury oraz przy wykorzystaniu technik manualnych, * Minimalne narzędzia jakie Wykonawca musi wykorzystać do przeprowadzenia testów zewnętrznych:   + Nmap   + Nessus Professional   + OpenVAS   + MetaSploit   + Foca   + Maltego   + Skrypty I narzędzia autorskie w Kali linux,   + Skrzypty I narzędzia autorskie powershell do enumeracji infrastruktury Microsoft Windows, | SPEŁNIA TAK /NIE |
|  |  | * Zamawiający wymaga, aby Wykonawca posiada potencjał osobowy niezbędny do wykonania zamówienia. Zamawiający wymaga aby osoby testujące łącznie posiadały poniższe certyfikaty: * Offensive Security Certified Professional (OSCP); * Certified Information Systems Security Professional (CISSP); * Certified Security Analyst (ECSA); * Wep Application Penatration Tester (eWPT); * Certified Professional Penetration Tester (eCPPT); * Certyfikat ISO 9001 oraz 27001 w szczególności w zakresie usług związanych z cyberbezpieczeństwem.   **Certyfikaty należy załączyć do oferty** | SPEŁNIA TAK /NIE |

## 3 SZKOLENIE BUDUJĄCE ŚWIADOMOŚĆ CYBERZAGROŻEŃ I SPOSOBÓW OCHRONY DLA PRACOWNIKÓW URZĘDU W FORMIE DOSTĘPU DO PLATFORMY SZKOLENIOWEJ

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne)** | **Oferowane parametry** |
|  | Charakterystyka ogólna | Platforma szkoleniowa zawierająca minimum 5 szkoleń, dostępnych w języku polskim w postaci prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego | SPEŁNIA TAK /NIE |
|  | Liczba uczestników: | Zamawiający przewiduje łączną liczbę uczestników szkoleń w ilości 120 | SPEŁNIA TAK /NIE |
|  | Dostępność platformy: | Platforma elearningowa musi być dostępna dla wszystkich uczestników przez 24h na dobę, przez okres 12 m-cy od daty podpisania umowy. | SPEŁNIA TAK /NIE |
|  | Szkolenie dostępne na platformie musi spełniać następujące wymogi | * 1. Być responsywne tzn. dostosować wyświetlanie do komputera oraz tabletu – w pionie i poziomie, i telefonu - w pionie i poziomie   2. „Zablokowane” tzn. uczestnik nie może przejść do części kursu zawierającej test sprawdzający wiedzę, bez zapoznania się z informacjami przedstawionymi na ekranie w postaci np. rozwijanych kart, okien pop-up, markerów, wyświetlonych pytań i odpowiedzi.   3. Być interaktywne tzn. muszą angażować uczestnika poprzez zapewnienie możliwości klikania, zapoznawania się z materiałami dodatkowymi, rozwijania i otwierania okien z informacjami oraz udzielania odpowiedzi na zadawane pytania.   4. Szkolenie musi się kończyć testem, w którym zostaną użyte pytania jednokrotnego wyboru, wielokrotnego wyboru, prawda/fałsz.   5. Test musi zakończyć się podsumowaniem wyniku uzyskanego przez uczestnika szkolenia w postaci wyniku procentowego, oraz informacji o uzyskaniu pozytywnej lub negatywnej oceny końcowej.   6. Uczestnik musi otrzymać informację zwrotną w postaci określenia na które pytania odpowiedział poprawnie, a na które błędnie.  1. Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:    * + - * Podstawy bezpiecznego internetu          * Bezpieczeństwo poczty          * Załączniki w poczcie elektronicznej          * Ochrona przed złośliwym oprogramowaniem          * Bezpieczeństwo danych osobowych RODO/GDRP          * Bezpieczne hasła i menedżery haseł          * Bezpieczeństwo urządzeń mobilnych          * Uwierzytelnianie wieloskładnikowe (MFA)          * Bezpieczna praca zdalna          * Bezpieczna praca w biurze          * Zagrożenia w mediach społecznościowych          * Ochrona przed phishingiem          * Socjotechnika – metody i techniki manipulacji człowiekiem          * Zakupy w internecie 2. Dedykowana platforma dostarczająca raporty obejmujące minimum: 3. liczbę wizyt na platformie w podziale na użytkownika i wszystkich użytkowników, 4. czas spędzony platformie w podziale na użytkownika i wszystkich użytkowników, 5. czas spędzony w kursie z opcją filtrowania po kursie, kohorcie, użytkowniku, 6. lista nieaktywnych użytkowników 7. rozkład czasowy korzystania użytkowników z platformy w ujęciu tygodniowym i 24 godzinnym 8. przegląd ocen w kursie z opcją filtrowania po kohortach, kursie, użytkowniku. 9. Popularność kursów na platformie w ujęciu zapisów, odwiedzin kursantów,   Wszystkie powyższe raporty muszą być prezentowane graficznie np.: tabela, lista, wykres oraz umożliwiać pobranie danych w formie pliku, np.: PDF lub JPG lub SVG.   1. Udostępniona platforma musi zostać dostosowana graficznie do layoutu Zamawiającego w zakresie minimalnym tj:  * logo i favicon, * wpisy w menu głównym, * zmiany treści stopki, * czcionki nagłówków i tekstów, * kolorystyka przycisków, * strony z treściami zgód (RODO, marketing) wymaganymi przy pierwszym logowaniu * stronę logowania do platformy (tło, logo). * jeśli zajdzie potrzeba stworzymy stronę główną platformy widoczną dla kursanta   przed zalogowaniem się do platformy.   * Zmiany wyglądu i treści wiadomości powitalnych wychodzących z platformy (logo, kolor tła, opis, czcionka, stroka emaila), | SPEŁNIA TAK /NIE |
|  | Wymagania: | * Środowisko pracy: Platforma e-learningowa musi być dostępna z poziomu przeglądarek internetowych Firefox, Chrome, Edge dla systemów Windows 10 / 11 w aktualnych wersjach; * Zasady działania pomocy technicznej: Zgłoszenia pomocy technicznej i komunikacja z Wykonawcą będą przyjmowane w języku polskim w trybie 24x7 przez funkcję chat dostępną na platformie oraz infolinię w języku polskim 24x7. Czas reakcji Wykonawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w polu chat.   **SLA – gwarantowany poziom świadczenia usług:**   * Dostępność platformy – na poziomie minimum 99,8% przez cały okres realizacji zamówienia; * Nielimitowany transfer danych; * Codzienna kopia zapasowa danych - przetrzymywana 28 dni * Platforma zabezpieczona certyfikatem SSL; * Minimalna ilość łącznych dostępów uczestników do platformy w tym samym czasie na poziomie 100%; * Zobowiązania Wykonawcy: * Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia;   **Dostępność platformy:**  Platforma elearningowa musi być dostępna dla wszystkich uczestników przez 24h na dobę. | SPEŁNIA TAK /NIE |

## 4 SZKOLENIA Z TESTAMI SOCJOTECHNICZNYMI DLA PRACOWNIKÓW URZĘDU

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne) Oferowane parametry** |  |
|  | Charakterystyka ogólna | 1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników administracyjnych, które zostaną poprzedzone testami socjotechnicznymi. 2. Dla każdej grupy uczestników szkoleń w każdym z cyklów szkoleniowych z osobna Zamawiający przewiduje ilość godzin szkolenia w wymiarze nie mniej niż 2 godziny; 3. Planowane terminy szkoleń: Zamawiający planuje przeprowadzenie szkoleń wz podziałem na 5 grup/y pracowników nie większe niż 20 osób; 4. Po podpisaniu umowy z Wykonawcą Zamawiający dopuszcza rotacje liczby uczestników podczas każdego cyklu szkoleniowego; 5. Szkolenia odbywać się będą w dni robocze od poniedziałku do piątku w godzinach 7:30 – 15:30 6. Szkolenie stacjonarne z zakresu cyberbezpieczeństwa skierowane do pracowników urzędu obejmujące co najmniej następujące obszary: a. wprowadzenie do cyberbezpieczeństwa:    * 1. czym jest cyberbezpieczeństwo;      2. kluczowe zagadnienia związane z cyberbezpieczeństwem;      3. przegląd statystyk i trendów w cyberbezpieczeństwie.   b. typy zagrożeń w cyberprzestrzeni:   * + 1. malware (wirusy, trojany, robaki itp.);     2. ataki typu phishing i spear phishing;     3. ataki DDoS;     4. ataki ransomware;     5. zagrożenia związane z sieciami społecznościowymi.   c. zasady bezpieczeństwa i praktyki:   * + 1. zarządzanie hasłami i uwierzytelnianie wieloskładnikowe;     2. zasady bezpieczeństwa e-mail;     3. bezpieczeństwo w sieciach bezprzewodowych;     4. bezpieczne przeglądanie internetu;     5. backup i odzyskiwanie danych.   d. reagowanie na incydenty i planowanie awaryjne:   * + 1. jak zidentyfikować i zgłosić incydent związany z cyberbezpieczeństwem;     2. zasady reagowania na incydenty;     3. planowanie awaryjne i kontynuacja działalności;     4. przegląd realnych przypadków naruszeń bezpieczeństwa  1. Zamawiający przewiduje przeprowadzenie testów socjotechnicznych z minimum 7 dniowym wyprzedzeniem, przed potwierdzonym terminem szkoleń dla pracowników urzędu. 2. Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi. 3. Testy muszą składać się z następujących faz:    1. Rozpoznanie (biały wywiad, obserwacja pracy pracowników).    2. Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy).    3. Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary). 4. Testy muszą być przeprowadzone za pomocą aktualnych narzędzi, wykorzystujących najnowsze możliwości w zakresie symulacji złośliwych kampanii socjotechnicznych. 5. Zakres testów:    1. Próba wyrywkowego przeprowadzenia testów socjotechnicznych za pomocą e-maila - próba będzie polegała na wysłaniu wiadomości e-mail na adresy służbowe pracowników Organizacji i przeprowadzeniu ataku socjotechnicznego.    2. Przygotowane przez testerów wiadomości muszą odpowiadać realnym atakom, realizowanym aktualnie przez przestępców. Wykonawca musi uwzględnić:       1. Ataki typu phishing,       2. Ataki typu spear phishing       3. Phishing typu whaling       4. Phishing przez klonowanie       5. Angler phishing    3. Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email):       1. otwieranych wiadomości,       2. otwieranych stron za pomocą linków umieszczonych w wiadomościach,       3. podawanych poświadczeń na stronach mających na celu wyłudzanie informacji, przygotowanych przez testerów,       4. pobieranie plików w popularnych formatach, takich jak „docx.”, czy „xlsx”,       5. otwierania plików w popularnych formatach, takich jak „docx.”, czy „xlsx”. | SPEŁNIA TAK /NIE |
|  | Wymagania wobec Wykonawcy | * Wykonawca oddeleguje do realizacji zadania prelegenta posiadającego certyfikat Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001 * Wykonawca przeprowadzi szkolenia w języku polskim; * Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia * W ramach organizacji każdego z cykli szkoleń Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników obejmujące szczegółowy zakres merytoryczny w wersji papierowej. * W ramach szkoleń Wykonawca zapewni dokumentację wszystkich szkoleń:  1. Listy obecności uczestników szkoleń; 2. Listy odbioru certyfikatów o ukończonych szkoleniach; 3. Dzienniki szkoleń zawierające informacje na temat przebiegu oraz o zakresie merytorycznym szkoleń, podpisane przez osobę prowadzącą szkolenia; 4. Dokumentację fotograficzną z przeprowadzonych szkoleń (forma elektroniczna);  * Wykonawca zobowiązuje się w terminie 5 dni od dnia podpisania umowy dostarczyć Zamawiającemu:  1. Proponowane terminy szkoleń; 2. Szczegółowy zakres merytoryczny szkoleń; 3. Harmonogram szkoleń;  * Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek do sporządzonej dokumentacji zgodnie z sugestiami Zamawiającego na każdym etapie realizacji zamówienia; * Certyfikat ISO 9001 oraz 27001 w szczególności w zakresie raz szkoleń związanych z cyberbezpieczeństwem * Certyfikat ISO 22301 | SPEŁNIA TAK /NIE |
|  | Symulator zagrożeń internetowych.  Warunki ogólne | Wykonawca podczas szkoleń zapewni dostęp do nowoczesnej platformy w formie strony www dostępnej w standardzie WCAG 2.1 – symulator zagrożeń Szkolenia obędą się z wykorzystaniem komputerów przenośnych – będących własnością Zamawiającego.  Symulator musi być narzędziem umożliwiającym użytkownikowi w bezpieczny sposób sprawdzenie oraz poznanie typowych zagrożeń czyhających na użytkowników w Internecie.  Korzystanie z symulatora musi być całkowicie bezpieczne dla użytkownika końcowego (żadne z wpisywanych danych nie mogą być zapisywane i archiwizowane).  W symulatorze konieczne jest zaimplementowanie min. 8 scenariuszy (zagrożeń) popularnych przestępstw internetowych, z którymi użytkownicy mogą się spotkać podczas codziennego korzystania z Internetu. Pierwsze cztery dotyczące tzw. Phishing’u w różnych odsłonach, ((Phishing Clone, Phishing Spear, Phishing Spear Chat, Phishing Whaling) następny dotyczy oszustwa typu Pharming, dwa kolejne mają przedstawiać zasadę działania zagrożenia typu Malware, (Malware Post, Malware Email,) natomiast ostatni dotyczący certyfikatów SSL (Certificate Fraud Chat).  Wykonawca zobowiązany jest przekazać zamawiającemu dostępy do platformy na okres min 30 dni od daty szkolenia danej grupy, wraz z instrukcją obsługi. | SPEŁNIA TAK /NIE |
|  | Wymagania szczegółowe dla platformy Symulującej zagrożenia internetowe: | 1. **Moduł podstron (fałszywych witryn)** – moduł ten będzie umożliwiał tworzenie różnego rodzaju fałszywych witryn nakłaniających użytkowników do pobierania zainfekowanych załączników, podawania danych wrażliwych i/lub dokonywania płatności internetowych. 2. **Moduł czatu –** w module tym zaimplementowany zostanie czat z botami, namawiającymi do zakupów różnych produktów powodując wyłudzenie danych osobowych, numerów kart kredytowych itp. Itd. W module tym zostaną zaimplementowane opracowane scenariusze 3. **Moduł e-mail** – w module tym użytkownik będzie miał do przeglądnięcia kilka wiadomości e-mail przesłanych z różnych źródeł, wiadomości te będą zawierały linki bądź załączniki po kliknięciu których, zostanie uruchomiona akcja symulująca zachowanie się malware, np. blokada komputera (przeglądarki) na jakiś określony czas. Po kliknięciu załącznika „zainfekowanego” na ekranie powinna pojawić się informacja na temat, że twój komputer został zainfekowany, wykradliśmy twoje dane osobowe itd. Itp. W tym module należy również pokazać działanie tzw. szyfrującego wirusa, który po kliknięciu w załącznik szyfruje wszystkie pliki tekstowe, w tym przypadku symulator powinien pokazać przykład 4. **Moduł edukacyjny –** moduł zawierający szczegółowe informacje na temat występujących cyberprzestępstw. W szczególności powinien się skupić na phishingu, pharmingu oraz malware.  * Moduł ten powinien zawierać informacje na temat występowania oraz identyfikacji danego zagrożenia, sposobów zapobiegania, oraz informacji na temat, co użytkownik powinien w pierwszej kolejności zrobić, gdy zostanie już oszukany – czyli gdzie się zgłosić najpierw, jakie dane zabezpieczyć, zmienić hasła, czy zablokować karty płatnicze. * Materiały edukacyjne powinny być przedstawione w formie plików PDF przedstawiających, na co zwrócić szczególną uwagę podczas korzystania z portali społecznościowych, różnego rodzaju czatów, różnego rodzaju serwisów internetowych oraz odbierania wiadomości e-mail. * Moduł edukacyjny powinien być ściśle zintegrowany z pozostałymi modułami tj. Po przejściu każdego z opracowanych i zaimplementowanych w symulatorze scenariuszy powinna pojawić się informacja o tym jak i dlaczego użytkownik dał się oszukać i jakie to może mieć konsekwencje w późniejszym czasie.  1. **Moduł postów społecznościowych,** zawierający możliwe ataki phishingowe lub pharmingowe, w module postów społecznościowych będą znajdować się zarówno „rzeczywiste” posty niestanowiące zagrożenia jaki i posty z potencjalnym zagrożeniem. | SPEŁNIA TAK /NIE |

## 5 SZKOLENIA SPECJALISTYCZNE DLA KADRY ZARZĄDZAJĄCEJ URZĘDU Z ZAKRESU CYBERBEZPIECZEŃSTWA

|  |  |  |  |
| --- | --- | --- | --- |
| **L.P** | **Parametr** | **Charakterystyka (wymagania minimalne) Oferowane parametry** |  |
|  | Charakterystyka ogólna | 1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry zarządzającej urzędu tj 14 osób. 2. Szkolenie dla kadry zarządzającej z zakresu cyberbezpieczeństwa musi zawierać następującą tematykę:    1. Wstęp do bezpieczeństwa w cyberprzestrzenii;    2. Akty Prawne;    3. Krajowy System Cyberbezpieczeństwa;    4. Analiza ataków cybernetycznych;    5. Najpopularniejsze zagrożenia;    6. Przewodnik po metodach obrony instytucji;    7. Cyberbezpieczeństwo osobiste;    8. Postępowanie w pracy;    9. ABC higieny pracy w cyberprzestrzeni;    10. Bezpieczeństwo pracy zdalnej;    11. Ataki socjotechniczne - czyli niewinne „wyłudzanie” danych    12. Kampanie Phishingowe    13. Opłacalność ataków DoS/DDoS wymierzonych w konkretną instytucję    14. Aktualne zagrożenia wynikające z wojny w Ukrainie·    15. Przeprowadzenie testu wiedzy; | SPEŁNIA TAK /NIE |
|  |  | * 1. Wykonawca oddeleguje do realizacji zadania prelegenta posiadającego certyfikat Bezpieczeństwa Informacji zgodnie z normą PN-EN ISO 27001   2. Wykonawca przeprowadzi szkolenia w języku polskim;   3. Wykonawca wyda każdemu uczestnikowi szkolenia certyfikat o ukończeniu szkolenia   4. W ramach organizacji każdego z cykli szkoleń Wykonawca zapewni materiały szkoleniowe dla wszystkich uczestników obejmujące szczegółowy zakres merytoryczny w wersji papierowej.   5. W ramach szkoleń Wykonawca zapewni dokumentację wszystkich szkoleń:      1. Listy obecności uczestników szkoleń;      2. Listy odbioru certyfikatów o ukończonych szkoleniach;      3. Dzienniki szkoleń zawierające informacje na temat przebiegu oraz o zakresie merytorycznym szkoleń, podpisane przez osobę prowadzącą szkolenia;      4. Dokumentację fotograficzną z przeprowadzonych szkoleń (forma elektroniczna);   6. Wykonawca zobowiązuje się w terminie 5 dni od dnia podpisania umowy dostarczyć Zamawiającemu:      1. Proponowane terminy szkoleń;      2. Szczegółowy zakres merytoryczny szkoleń;      3. Harmonogram szkoleń;   7. Wykonawca zobowiązany jest do współpracy i konsultacji z Zamawiającym oraz do wprowadzania poprawek do sporządzonej dokumentacji zgodnie  z sugestiami Zamawiającego na każdym etapie realizacji zamówienia; |  |

**Niespełnienie któregokolwiek z wymaganych parametrów oraz wymagań co do nich wartości minimalnych spowoduje odrzucenie oferty bez dalszej jej oceny jako oferta niezgodna z warunkami zamówienia.**