**Opis Przedmiotu zamówienia:**

**Audyt Bezpieczeństwa i Diagnoza Cybrebezpieczeństwa**

|  |  |
| --- | --- |
| Komponent | Zakres prac |
| 1.  Audyt dokumentacji i procesów | **1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC)**  - wyznaczenie osoby do kontaktu - Art. 21 KSC  - przekazanie danych osoby wyznaczonej - Art. 22 pkt 5) KSC  - zapewnienie zarządzania incydentem - Art. 22 pkt 1) KSC  - zgłaszanie incydentu - Art. 22 pkt 2) Art. 23 KSC  - zapewnienie obsługi incydentu - Art. 22 pkt 3) KSC  - zapewnienie dostępu do wiedzy - Art. 22 pkt 4) KSC  - opracowanie, ustanowienie i wdrożenie SZBI - Par. 20 KRI  - monitorowanie i przegląd SZBI - Par. 20 KRI  - doskonalenie SZBI - Par. 20 KRI  - aktualizowanie regulacji wewnętrznych - Par. 20 pkt 1) KRI  - inwentaryzacja sprzętu i oprogramowania - Par. 20 pkt 2) KRI  - przeprowadzanie okresowych analiz ryzyka - Par. 20 pkt 3) KRI  - postępowanie z ryzykiem - Par. 20 pkt 3) KRI  - zarządzanie uprawnieniami - Par. 20 pkt 4), 5) KRI  - szkolenia i uświadamianie - Par. 20 pkt 6) KRI  - monitorowanie dostępu do informacji - Par. 20 pkt 7) a), b) KRI  - monitorowanie nieautoryzowanych zmian - Par. 20 pkt 7) b) KRI  - zabezpieczenie nieautoryzowanego dostępu - Par. 20 pkt 7) c) KRI  - ustanowienie zasad bezpiecznej pracy mobilnej - Par. 20 pkt 8) KRI  - zabezpieczenie informacji przed nieuprawnionym ujawnieniem - Par.20 pkt 9) KRI  - zabezpieczenie informacji przed nieuprawnioną modyfikacją - Par. 20 pkt 9) KRI  - zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem-Par. 20 pkt 9) KRI  - zawieranie w umowach serwisowych zapisów o bezpieczeństwie - Par. 20 pkt 10) KRI  - ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania - Par. 20 pkt 11) KRI  - aktualizowanie oprogramowania - Par. 20 pkt 12) a) KRI  - minimalizowanie ryzyka utraty informacji w wyniku awarii systemu - Par. 20 pkt 12) b) KRI  - ochrona systemu przed błędami - Par. 20 pkt 12) c) KRI  - stosowanie mechanizmów kryptograficznych w systemach - Par. 20 pkt 12) d) KRI  - zapewnienie bezpieczeństwa plików systemowych - Par. 20 pkt 12) e) KRI  - zarządzanie podatnościami systemów - Par. 20 pkt 12) f), g) KRI  - kontrola zgodności systemów z regulacjami - Par. 20 pkt 12) h) KRI  - zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok - Par. 20 pkt 14) KRI  **2.  Ocena wybranych aspektów bezpieczeństwa systemów informatycznych**  - dokumentacja potwierdzająca wykonane działania wskazanego w ustawie  - opis identyfikacji systemu informacyjnego wspierającego zadanie publiczne  - dokumentacja Systemu Informacyjnego wspierającego zadanie publiczne  - dokumentacja procesu zarządzania incydentami  - aspekty techniczne do weryfikacji)  **3.  Ocena dojrzałości wybranych procesów bezpieczeństwa**  - ochrona przed kodem szkodliwym  - ochrona sieci i połączeń  - ochrona urządzeń końcowych  - zarządzanie tożsamością i autoryzacją dostępu  - ochrona fizyczna systemów IT  - bezpieczeństwo urządzeń drukujących  - zarządzanie podatnościami  **4.  Opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny** |
| 2  Testy penetracyjne infrastruktury sieciowej | 1.  Przedstawienie założeń Audytu  Audyt wykonywany będzie w sposób manualny oraz automatyczny za pomocą specjalistycznych narzędzi oraz własnych skryptów przygotowanych na podstawie wiedzy i doświadczeń. Testy zostaną przeprowadzone w oparciu o OSSTMM (Open Source Security Testing Methodology Manual).    2.  Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci    3.  Skanowanie sieci - rekonesans sieci  Sprawdzenie jakie hosty są w sieci widoczne, ile ich jest, usługi jakie są uruchomione na hostach, jakie systemy operacyjne działają na wykrytych hostach. W szczególności ten etap polega na:  - skanowaniu sieci w poszukiwaniu wszystkich podłączonych hostów  - wykryciu czy jest dostęp do innych podsieci z danej podsieci  - wykryciu usług działających na hostach podłączonych do sieci  - wykryciu podatności na wybranych hostach w sieci  4.  Skanowanie będzie powtórzone dla każdej wskazanej przez zamawiającego sieci  Przeprowadzenie skanowania w prawidłowo działającej sieci nie powinno mieć negatywnego wpływu na działanie sieci. Po przeskanowaniu sieci wraz z Zamawiającym zostanie wybrana pula hostów do dalszego badania.  5. Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy  - weryfikacja występowania luk bezpieczeństwa dla konkretnych usług  - w zależności od wykrytej usługi weryfikacja haseł  - weryfikacja dostępu użytkowników do odpowiednich usług  - weryfikacja możliwości dostępu do usługi  - weryfikacja luk bezpieczeństwa w systemie operacyjnym  - weryfikacja luk bezpieczeństwa w oprogramowaniu firm trzecich  6.  Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy  - weryfikacja haseł w usługach umożliwiających logowanie  7.  Sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł  8.  Weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych  9.  Weryfikacja zabezpieczeń urządzeń sieciowych  - badanie odporności switchy na ataki sieciowe  - weryfikacja zabezpieczeń monitoringu wizyjnego  10.  Testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej  - weryfikacja pod kątem dostępu  - weryfikacja pod kątem zabezpieczeń  - wykrycie możliwości przechwycenia haseł  - w przypadku przechwycenia hasła - weryfikacja pod katem możliwości złamania hasła  11.  Zdalne testy adresów publicznych  12.  Badanie ankietowe  Badanie ankietowe pracowników działu IT oraz pracowników Zamawiającego z wiedzy o bezpieczeństwie sieci i procedurach IT stosowanych przez Zamawiającego. Grupa ankietowanych pracowników zostanie ustalona podczas Audytu. |
| Opis Raportu | 13.  Wykonanie raportu zawierającego  - opis wszystkich elementów, które zostały poddane audytowi  - podział podatności ze względu na ryzyko:  - wysoki  - średni  - niski  - wskazanie zaleceń, rekomendacji, najlepszych praktyk - dla każdej znalezionej podatności  - wylistowanie wszystkich podatności ze względu na ryzyko:  - wysoki  - średni  - niski  - określenie bezpieczeństwa informatycznego w organizacji poprzez wskazanie ilości i rodzaju znalezionych podatności |
| Dodatkowe wymagania: | Dostarczyć do Zamawiającego poufny dokument prezentujący wyniki testów i opisujący wszystkie spostrzeżenia oraz zalecenia zmian konfiguracji systemów informatycznych.  Dostarczyć Zamawiającemu wypełniony formularz diagnozy (przeprowadzonej przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu). |
| Termin wykonania zamówienia | III.  Termin wykonania zamówienia: 30 dni od podpisania umowy.  IV. Czas realizacji usługi  - Zdalnie do 4 dni  - Na miejscu do 5 dni |
| Odbiór robót: | 1.  Odbiór przez Zamawiającego, nastąpi w ciągu 2 dni od przekazania dokumentów audytu i diagnozy cyberbezpieczeństwa wraz ze zgłoszeniem zakończenia prac.  2.  Przed podpisaniem protokołu odbioru, osoba pełniąca nadzór nad zamówieniem po stronie Zamawiającego, ma prawo skontrolować postęp wykonywanych prac.  3.  Podstawę wystawienia faktury, stanowił będzie obustronnie podpisany bez uwag protokół odbioru. |
| Wynagrodzenie: | 1. Wynagrodzenie za wykonanie przedmiotu zamówienia obejmuje wszelkie koszty związane z jego realizacją, w tym koszt dojazdu, zakwaterowania itp.  2. Wynagrodzenie płatne będzie w terminie 30 dni od dnia złożenia u Zamawiającego prawidłowej faktury VAT. |