ZAŁĄCZNIK NR 1B

Opis Przedmiotu Zamówienia

Część 2

Diagnoza Cyberbezpieczeństwa

Projekt „Cyfrowa Gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020.

Specyfikacja techniczna / funkcjonalna przedmiotu zamówienia

Spis treści

Wstęp

Niniejszy dokument określa minimalne wymagania dla dostawy infrastruktury sprzętowej i oprogramowania, wykonania: diagnozy cyberbezpieczeństwa (audytu) w ramach realizacji projektu pn.: „Cyfrowa Gmina”. Zakup jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia, dotyczący realizacji projektu grantowego „Cyfrowa Gmina” dla Gminy Sędziejowice o numerze POPC.05.01.00-00-0001/21-00.

1. Diagnoza Cyberbezpieczeństwa – 1 szt.

Lp.	Nazwa komponentu	Wymagane minimalne parametry audytu
1	2	3
Audyt cyberbezpieczeństwa		
1.	**Typ**	Wykonanie audytu diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do dokumentacji konkursowej - Cyfrowa Gmina. Wynikiem przeprowadzenia diagnozy musi być raport dotyczący audytowanego środowiska oraz wypełnienie formularza diagnozy i dostarczenia go za pomocą elektronicznej skrzynki podawczej ePUAP do NASK - PIB na adres skrzynki: /NASK-Instytut/SkrytkaESP (akronim/temat: cyfrowa.gmina.diagnoza.cyber)
2.	**Plan audytu**	Audyt musi składać się z minimum: 1. Audyt dokumentacji i procesów: - ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC) - ocena wybranych aspektów bezpieczeństwa systemów informatycznych - ocena dojrzałości wybranych procesów bezpieczeństwa - opracowanie raportu z audytu oraz uzupełnienie arkusza do oceny 2. Testy penetracyjne infrastruktury sieciowej - Weryfikacja dokumentacji sieci, topologii sieci, kluczowych elementów sieci - skanowanie sieci, rekonesans sieci (skanowanie musi zostać powtórzone dla każdej wskazanej przez Zamawiającego sieci) - skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), który zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy - sprawdzenie możliwości wylistowania użytkowników oraz zdobycia haseł - weryfikacja możliwości uzyskania dostępu do zasobów współdzielonych - weryfikacja zabezpieczeń urządzeń sieciowych - testy sieci bezprzewodowej oraz weryfikacja zabezpieczeń sieci bezprzewodowej - wykonanie raportu zawierającego minimum: ● 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 - Wsparcie poaudytowe - Udzielenie informacji na temat audytowanych elementów wynikających z raportu. Czas na zapoznanie się z raportem i zadawanie pytań odnośnie raportu.
3.	**Wymagania dla audytora/-ów**	Audyt musi zostać przeprowadzony przez osobę posiadająca uprawnienia wskazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu: 1. Certified Internal Auditor (CIA); 2. Certified Information System Auditor (CISA);

		3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób; 4. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób; 5. Certified Information Security Manager (CISM); 6. Certified in Risk and Information Systems Control (CRISC); 7. Certified in the Governance of Enterprise IT (CGEIT); 8. Certified Information Systems Security Professional (CISSP); 9. Systems Security Certified Practitioner (SSCP); 10. Certified Reliability Professional; 11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert

2. Równoważność rozwiązań

Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym przez Zamawiającego. Wykonawca oferując rozwiązanie równoważne do opisanego powyżej jest zobowiązany wykazać (udowodnić) równoważność w zakresie wskazanych parametrów, które muszą być na poziomie nie gorszym niż parametry wskazane przez Zamawiającego - Wykonawca musi wykazać (udowodnić), iż proponowane rozwiązanie w równoważnym stopniu spełnia wymagania określone w SWZ, w szczególności w zakresie parametrów. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do określonego wyrobu, źródła, znaków towarowych, patentów czy pochodzenia lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę – należy przyjąć, że Zamawiający podał taki opis ze wskazaniem na typ i dopuszcza składanie ofert równoważnych, w szczególności o parametrach technicznych, użytkowych, funkcjonalnych i jakościowych nie gorszych niż te, podane w opisie przedmiotu zamówienia. Ilekroć Zamawiający przy opisie przedmiotu zamówienia powołuje się na normy, aprobaty, specyfikacje techniczne czy systemy odniesienia Zamawiający dopuszcza rozwiązania równoważne. Jeżeli w opisie przedmiotu zamówienia znajdują się jakiekolwiek odniesienia do wielkości fizycznych ciała lub zjawiska, którą można określić ilościowo, czyli zmierzyć za pomocą jednostki miary (o ile nie wskazano inaczej) – należy przyjąć, iż jako równoważne Zamawiający uzna ofertę, która uwzględni wymiary wraz z dopuszczonymi odchyleniami od wymiarów podanych w zapytaniu ofertowym mieszczące się w granicach tolerancji określonych normą/standardem, dla której/którego wypracowano system normalizacji i certyfikacji na poziomie co najmniej międzynarodowym. Norma/standard musi być obowiązujący wg przepisów prawa na dzień wyceny. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego jest obowiązany wykazać (udowodnić), że oferowany przez niego produkt spełnia wymagania określone przez Zamawiającego w SWZ..