zał. numer 2 do zapytania

OPIS PRZEDMIOTU ZAMÓWIENIA

Wymagania dla usługi przeprowadzenia audytów łączonych SZBI oraz KRI & UoKSC (audyt początkowy oraz audyt końcowy) dla UG Piątnica oraz jednostek podległych: Centrum Usług Samorządowych, Ośrodka Pomocy Społecznej w Piątnicy, 7 placówek edukacyjnych (Zespół Szkolno-Przedszkolny w Piątnicy, Szkoła Podstawowa w Kisielnicy, Dobrzyjałowie, Drozdowie, Olszynach, Rakowo-Boginie i Jeziorku)

WYMAGANIA OGÓLNE:

1. Wykonawca przeprowadzi w roku 2025 i 2026 audyt 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), zwany dalej „audytem KRI".
2. Zakres audytu systemu bezpieczeństwa informacji każdorazowo obejmie zgodność z kryteriami zawartymi w § 19 ust. 2 ww. rozporządzenia KRI.
3. Raport z audytu KRI zostanie każdorazowo podpisany przez audytora dokonującego audyt KRI -i dostarczony do Zamawiającego w formie elektronicznej.
4. Audyt KRI oraz 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
   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 lub równoważnej.
5. 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 8 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
6. Wypełnienie ankiety dojrzałości cyberbezpieczeństwa polegać będzie wypełnieniu przez Wykonawcę kolumn H, I z arkusza „Ankieta" 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 podpisu elektronicznego i dostarczona do Zamawiającego w formie elektronicznej.
7. Jednostki samorządu terytorialnego oraz ich jednostki podległe, które biorą udział w projekcie „Cyberbezpieczny Samorząd" są zobowiązane do przesłania do NASK raportu z audytu KRI oraz wypełnionej ankiety dojrzałości cyberbezpieczeństwa. Niezwłocznie po ich przekazaniu przez Wykonawcę dokumenty te zostaną przekazane przez Zamawiającego do Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (NASK) za pośrednictwem platformy ePUAP. Dane z tej dokumentacji przekazane przez JST do NASK posłużą do opracowania raportu na temat stanu bezpieczeństwa systemów jednostek samorządowych. Wykonawca jest zobowiązany mieć na uwadze także powyżej wskazany cel przeprowadzenia zamówienia i jego przeznaczenie.
8. Wykonawca zrealizuje zamówienie w oparciu o dokumentację, którą Zamawiający dysponuje niezależnie od realizacji przedmiotu umowy i o wyjaśnienia udzielane przez Zamawiającego. W szczególności realizacja

przedmiotu umowy przez Wykonawcę nie może być uwarunkowana wytwarzaniem lub uzupełnianiem dokumentów i opracowań przez Zamawiającego w związku z realizacją przedmiotu umowy, tj. Zamawiający nie może być zobowiązany do wypełniania ankiet, kwestionariuszy, sporządzania notatek itp., a informacje niezbędne Wykonawcy do wykonania przedmiotu umowy mogą być pozyskiwane wyłącznie w postaci materiałów źródłowych i wywiadu bezpośredniego.

9. Zamawiający dopuszcza prowadzenie prac związanych z: analizą dokumentacji, opracowaniem dokumentacji i polityk, opracowania raportów poza siedzibą Zamawiającego. Zamawiający nie dopuszcza prowadzenia instruktaży, konsultacji, audytów, analiz stanu istniejącego i określenie stanu faktycznego zabezpieczeń technicznych w formule zdalnej, tj. w postaci on-line lub innej poza siedzibami UG Piątnica i jego jednostek organizacyjnych

Przedmiot Zamówienia:

AUDYT POCZĄTKOWY łączony SZBI oraz KRI & UoKSC stanowi kluczowy element w ramach projektu Cyberbezpieczny Samorząd, a jego celem jest dokonanie wstępnej oceny obecnego stanu bezpieczeństwa informacji u Zamawiającego, w tym identyfikacja wszelkich zagrożeń, słabości, luk w zabezpieczeniach itd. Na podstawie wyników audytu należy zweryfikować braki i obszary wymagające poprawy, co kluczowe jest dla skutecznego wdrożenia działań w ramach projektu. Audyt początkowy niezbędny jest dla Zamawiającego do oceny zgodności z normami i standardami dotyczącymi zarządzania bezpieczeństwem informacji, a jego wyniki stanowią fundament do opracowania dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

AUDYT KOŃCOWY łączony SZBI & UoKSC ma wykazać efektywność wdrożonych działań i weryfikację czy zidentyfikowane w audycie początkowym słabości i luki zostały skutecznie zlikwidowane, a także czy nowo wdrożone procedury i mechanizmy działają zgodnie z ich założeniami.
Zamawiający wymaga, aby audyt końcowy stanowił formalną ocenę funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji i weryfikację jego poprawności, funkcjonowania zgodnie z wymaganiami norm, przepisów prawnych oraz wewnętrznych polityk. Audyt końcowy jest także dla Zamawiającego niezbędny do zapewnienia, że Jednostka jest przygotowana do dalszego funkcjonowania zgodnie z wymogami cyberbezpieczeństwa, a ponadto jego uzasadnienie znajduje się w konieczności formalnego zamknięcia Projektu i jego ocenę.

Zamawiający wymaga, aby w ramach czynności audytowych Wykonawca przeprowadził kompleksowy test penetracyjny wraz z czynnościami audytowymi) infrastruktury IT Jednostek. Testy penetracyjne mają na celu identyfikację i ocenę nieznanych dotąd podatności. Testy te muszą być wykonane przez wykwalifikowanego pentestera i powinny obejmować szczegółową analizę zarówno zewnętrznych, jak i wewnętrznych komponentów systemu informatycznego.

Zamawiający wymaga, aby zakres testów penetracyjnych obejmował m.in.:

1. **Zewnętrzne testy penetracyjne infrastruktury IT:**
    - analiza topologii sieci na granicy z Internetem - szczegółowe zbadanie struktury sieci na styku z Internetem, z uwzględnieniem istniejących zabezpieczeń;
    - ocena mechanizmów ochronnych - sprawdzenie efektywności systemów zabezpieczeń, takich jak zapory sieciowe, IDS/IPS oraz inne urządzenia na granicy sieci;
    - wykrywanie publicznie dostępnych usług sieciowych - przeprowadzenie skanowania portów oraz usług dostępnych publicznie w celu zidentyfikowania potencjalnych punktów dostępu dla atakujących;

- identyfikacja wersji i typów publicznie dostępnego oprogramowania - ustalenie wersji oprogramowania, które jest widoczne z sieci publicznej, w celu określenia możliwych luk w zabezpieczeniach;
- próby wykorzystania wykrytych podatności - testowanie ryzyka poprzez wykorzystanie zidentyfikowanych luk bezpieczeństwa;
- zalecenia dotyczące wzmocnienia ochrony sieci brzegowej - przygotowanie zaleceń dotyczących wzmocnienia ochrony na granicy sieci lokalnej z Internetem.

2. **Wewnętrzne testy penetracyjne infrastruktury IT:**
   - ocena struktury sieci LAN**: Szczegółowa analiza wewnętrznej topologii sieci LAN, w tym rozmieszczenia urządzeń oraz zastosowanych mechanizmów ochrony;
   - testowanie wewnętrznych zabezpieczeń sieciowych - sprawdzenie izolacji urządzeń, segmentacji sieci oraz innych środków ochronnych stosowanych w sieci wewnętrznej;
   - analiza i monitoring ruchu sieciowego - przeprowadzenie dokładnego monitoringu ruchu sieciowego w poszukiwaniu nietypowych wzorców mogących świadczyć o naruszeniu bezpieczeństwa;
   - skanowanie portów i usług w sieci LAN - identyfikacja usług i aplikacji działających w sieci wewnętrznej poprzez skanowanie portów TCP/UDP;
   - wykrywanie aktywnych urządzeń w sieci - identyfikacja i analiza urządzeń podłączonych do sieci lokalnej w celu oceny potencjalnych zagrożeń;
   - eksploatacja zidentyfikowanych podatności w sieci LAN - przeprowadzenie prób wykorzystania słabości w sieci wewnętrznej w celu oceny ryzyka;
   - ocena procedur tworzenia i odzyskiwania kopii zapasowych - przegląd skuteczności procedur backupu i przywracania danych;
   - rekomendacje dla poprawy bezpieczeństwa wewnętrznej sieci LAN - przygotowanie szczegółowych zaleceń dotyczących zwiększenia poziomu zabezpieczeń sieci lokalnej.

3. **Audyt bezpieczeństwa serwisów WWW:**
   - sprawdzenie aktualności serwera HTTP oraz systemu CMS - ocena zgodności wersji oprogramowania serwerowego oraz systemu CMS z najnowszymi standardami bezpieczeństwa, z naciskiem na wykrywanie znanych luk;
   - ocena bezpieczeństwa komunikacji internetowej - analiza stosowanych certyfikatów X.509, wersji protokołu TLS oraz metod kryptograficznych, zapewniających poufność i integralność transmisji danych przez Internet.

4. **Audyt bezpieczeństwa serwisów pocztowych:**
   - analiza mechanizmów SPF, DKIM i DMARC - ocena poprawności implementacji mechanizmów SPF, DKIM oraz DMARC, mających na celu ochronę przed fałszerstwami wiadomości e-mail;
   - ocena zabezpieczeń TLS w komunikacji e-mailowej - sprawdzenie czy mechanizmy szyfrowania TLS zostały poprawnie wdrożone w celu zabezpieczenia komunikacji pocztowej.

5. **Raport z przeprowadzonych testów i audytów:**
   - dokumentacja wykonanych prac - szczegółowy raport zawierający opis zastosowanej metodologii, użytych narzędzi oraz zakresu wykonanych testów i analiz;

- analiza wyników testów penetracyjnych - przedstawienie wyników testów, wraz z identyfikacją wykrytych podatności i oceną związanego z nimi ryzyka;
- zalecenia i wnioski - opracowanie rekomendacji dotyczących naprawy wykrytych problemów oraz strategii mających na celu podniesienie poziomu bezpieczeństwa;
- szczegółowa analiza technicznych zabezpieczeń - ocena oraz omówienie stanu zabezpieczeń serwisów WWW, serwisów pocztowych, sieci LAN i połączeń z Internetem, wraz z zaleceniami dotyczącymi utrzymania wysokiego poziomu bezpieczeństwa.

Opracowanie raportu z audytu wskazującego wykryte podatności oraz błędy wraz rekomendacjami działań naprawczych i korygujących oraz uzupełnienie załącznika nr 6 do Regulaminu Konkursu Grantowego pn. „Cyberbezpieczny Samorząd" – ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego.

Z kolei wsparcie poaudytowe, które polegać ma m.in. na: udzielanie informacji na temat audytowanych elementów wynikających z raportu. Czas dla klienta na zapoznanie się z raportem i zadawanie pytań odnośnie raportu min. 6 miesięcy od przeprowadzenia audytu i przedstawieniu raportu.

6. 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 8 - Ankieta Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego i Jednostkach Podległych).
7. Na podstawie przeprowadzonej analizy dokumentacji oraz audytu bezpieczeństwa, Wykonawca jest zobowiązany przedstawić pisemny raport zawierający wszystkie wyniki, wnioski wraz z propozycją zmian w zakresie spełnienia wymagań Rozporządzenia KRI. W raporcie muszą zostać uwzględnione wszystkie wyniki cząstkowe z audytowanych obszarów. Spełnienie poszczególnych wymagań zostanie określone w trzyelementowej skali: 1) spełnione – oznacza, że wymaganie normy zostało całkowicie wdrożone, 2) częściowo spełnione – może zaistnieć, czy dany obszar został udokumentowany (opracowano stosowną procedurę lub przygotowano inne zabezpieczenie), ale wybrany mechanizm nie został skutecznie wdrożony (np. zdefiniowano strefy bezpieczeństwa, ale system kontroli dostępu nie funkcjonuje poprawnie); najczęstszym przypadkiem oznaczenia wymagania jako „częściowo spełnionego" jest nieskuteczne wdrożenie procedury (nie przestrzeganie zapisów procedury przez pracowników), 3) niespełnione – wymaganie niespełnione oznacza, że nie zostało ono w ogóle zidentyfikowane przez podmiot (podmiot nie jest świadomy danego zagrożenia) lub nie podjęto żadnych działań, aby wdrożyć odpowiednie mechanizmy zabezpieczające.

Równoważność rozwiązań

1. 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.
2. Zamawiający informuje, że tam, gdzie w Zapytaniu oraz załącznikach opisał przedmiot zamówienia przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charak-

teryzuje produkty dostarczane przez konkretnego Wykonawcę, co mogłoby doprowadzić do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, Zamawiający dopuszcza rozwiązanie równoważne opisywanym 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.

3. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać, że oferowane przez usługi spełniają wymagania określone przez Zamawiającego. W takiej sytuacji Zamawiający wymaga złożenia stosownych dokumentów, uwiarygodniających te rozwiązania.
4. 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.
5. Za równoważne do normy PN-EN ISO/IEC 27001:2023 Zamawiający uzna inne normy dotyczące międzynarodowego standardu w zakresie bezpieczeństwa informacji obejmujące wymagania normy PN-EN ISO/IEC 27001:2023 określone w rozdziałach 4-10 tej normy.

Niniejszy opis przedstawia minimalny zakres wymagań dla przeprowadzenia kompleksowych testów penetracyjnych oraz audytów bezpieczeństwa IT, które mają na celu wszechstronną ocenę stanu bezpieczeństwa informatycznego Jednostek Zamawiającego.