Załącznik 2a

SZCZEGOŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ I – DOKUMENTACJA SZBI

Opracowanie i wdrożenie pełnej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), w tym między innymi wprowadzenie polityk bezpieczeństwa informacji (PBI), analizy ryzyka (w tym opracowanie i wdrożenie metodyk) np. procedury: obsługi incydentów ciągłości działania i zarządzania kryzysowego stosowania kryptografii i szyfrowania kontroli dostępu bezpieczeństwa pracy zdalnej używania urządzeń mobilnych pełnego rejestru czynności przetwarzania upoważnień dla Urzędu Gminy Czorsztyn, Zakładu Gospodarki Komunalnej w Maniowach, Gminnego Ośrodka Pomocy Społecznej w Maniowach.
Etap I – Audyt zerowy;
Etap II – Analiza ryzyka;
Etap III – Opracowanie dokumentacji SZBI;
Etap IV – Wdrożenie systemu Zarządzania Bezpieczeństwem Informacji;

Opracowanie dokumentacji SZBI ma być zgodne z:
- normami ISO/IEC 27001, ISO 22301,
- Rozporządzeniem 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. poz. 773),
- Ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn.zm.),
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.),
- Dyrektywa 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) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

CZĘŚĆ II – PRZEPROWADZENIE AUDYTÓW

Przeprowadzenie Audytu KRI/ouKSC poprzedzonego skanami podatności infrastruktury informatycznej urzędu, które pozwolą na zminimalizowanie ryzyka poważnych incydentów ataków hakerskich nieautoryzowanego dostępu do sieci w Urzędzie Gminy Czorsztyn Przeprowadzenie audytów SZBI zgodnie z wymaganiami przepisów prawa oraz

przeprowadzenie audytu dotyczącego wymagań w zakresie rozliczenia projektu „Cyberbezpieczny Samorząd” w Urzędzie Gminy Czorsztyn.

CZĘŚĆ III - SZKOLENIA

Szkolenia z zakresu cyberbezpieczeństwa dla kadry JST istotnych z punktu widzenia wdrażanej polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji (Rozporządzenia ogólnego RODO Rozporządzenia o Krajowych Ramach Interoperacyjności oraz Ustawy o Krajowym Systemie Cyberbezpieczeństwa, ze szczególnym uwzględnieniem zagadnień analizy ryzyka, oraz wymagań Dyrektywy NIS 2 oraz podstawowe szkolenia budujące świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST, potwierdzone certyfikatami ukończenia szkoleń dla Urzędu Gminy Czorsztyn, Zakładu Gospodarki Komunalnej w Maniowach, Gminnego Ośrodka Pomocy Społecznej w Maniowach Profesjonalne szkolenie z administrowania i zarządzania urządzeniami UTM i FortiSwitch dla Informatyka celem podniesienia kompetencji w administrowaniu, tymi systemami, a co za tym idzie zwiększeniem poziomu cyberbezpieczeństwa w JST.

Platforma szkoleniowa, z testami fałszywych maili (phishing) szkolenie stacjonarne dla pracowników: Urzędu Gminy Czorsztyn z/s w Maniowach, Gminnego Ośrodka Pomocy Społecznej w Maniowach, Zakładu Gospodarki Komunalnej w Maniowach, Szkoły Podstawowej im. Tetmajera w Maniowach, Szkoły Podstawowej w Sromowcach Wyżnych, Szkoły Podstawowej w Sromowcach Niżnych, Zespołu Szkolno Przedszkolnego w Kluszkowcach) szkolenia z zakresu cyberbezpieczeństwa powiązane z testami socjotechnicznymi dla kadry JST.
Szkolenie należy przeprowadzić w formie stacjonarnej dla 50 osób, w grupach po 10-15 osób. Każde szkolenie winno trwać minimum 4-5 godzin.

Wymagania ogólne dla platformy edukacyjnej:
Przedmiotem zadania jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy.

Usługa musi zawierać:

1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware

- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła
- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Socjotechnika stosowana
- ✓ Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:
a) z linkiem prowadzącym do stronnym internetowej,
b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.
3. dedykowaną platformę dostarczającą raporty obejmujące minimum:
a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:
- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,

- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń (2 zmiany miesięcznie) lub liczby użytkowników (nie więcej niż 10% zmian w okresie trwania usługi).

Wymagania dodatkowe:
Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. *Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.*
Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.