SZCZEGOŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

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. Szkolenie z zakresu Cyberbezpieczeństwa musi być tożsame z opracowaną przez Zamawiającego dokumentacją SZBI, w tym 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).

W związku z zapewnieniem zgodności z powyższymi, oraz fakt że szkolenie odnosi się do Systemu Zarządzania Bezpieczeństwem Informacji, który jest ściśle powiązany z normą ISO 27001, Zamawiający wymaga, aby osoba prowadząca szkolenie posiadała:

- Certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001;

- Certyfikat audytora wiodącego Systemu Zarządzania Ciągłością Działania wg normy PN-EN ISO 22301:2020-04.

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.

W ramach zadania należy także przeprowadzić w formie stacjonarnej profesjonalne szkolenie z zakresu cyberbezpieczeństwa min. 3 dni dla działu IT Urzędu Gminy – 1 osoba.

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.

<u>Usługa musi zawierać:</u>

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).

<u>Wymagania dodatkowe:</u>

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 certyfikat ISO 9001.

Profesjonalne szkolenie z zakresu FortiGate Administrator dla Informatyka Urzędu Gminy

Profesjonalne autoryzowane szkolenie FortiGate Administrator. Firma prowadząca szkolenie musi posiadać autoryzację edukacyjną firmy Fortinet w Polsce, a prowadzący szkolenie musi być certyfikowanym trenerem Fortinet – Fortinet Certified Trainer. Uczestnik musi otrzymać certyfikat potwierdzający zrealizowanie szkolenia, asygnowany przez Fortinet. Szkolenie musi być przeprowadzone w formie stacjonarnej, a plan szkolenia musi obejmować zagadnienia:

Plan szkolenia powinien zawierać :

• System and Network Settings

• Firewall Policies and NAT

• Routing

• Firewall Authentication

• Fortinet Single Sign-On (FSSO)

• Certificate Operations

• Antivirus

• Web Filtering

• Intrusion Prevention and Application Control

• SSL VPN

• IPsec VPN

• SD-WAN Configuration and Monitoring

• Security Fabric

• High Availability

• Diagnostics and Troubleshooting

• Język szkolenia - polski

Oferent wraz z ofertą zobowiązany jest przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Dodatkowo oferent zapewnia zamawiającemu udział w warsztatach technicznych stacjonarnych pozwalających na utrwalenie wiedzy oraz przetestowanie w bezpiecznym środowisku testowym nowych konfiguracji. Warsztaty musi prowadzić firma posiadająca specjalizację producenta w zakresie: Data center, Public Cloud Security.

Profesjonalne szkolenie z zakresu cyberbezpieczeństwa dla informatyka

Szkolenie musi trwać 4 dni w ramach którego użytkownik otrzymuje:

Prezentację ze szkolenia w formie PDF, Pakiet dokumentacji (format docx) do wykorzystania w swojej firmie:

- Przykładowa polityka bezpieczeństwa
- Procedura reagowania na incydent bezpieczeństwa
- Instrukcja umieszczania systemów w DMZ
- Możliwe zakresy testów bezpieczeństwa
- Linki do stron/narzędzi pokazywanych w trakcie szkolenia

Certyfikat ukończenia szkolenia (PDF).

Zapis filmowy szkolenia do końca 2025 roku.

Dostęp do platformy szkoleniowej.

Szkolenie musi zawierać poniższe zagadnienia:

- Podstawy rekonesansu infrastruktury IT

- W jaki sposób atakowane są firmy / użytkownicy – i jak temu zapobiec?

- Jak ransomware dostaje się do firm?

- Elementy bezpieczeństwa informacji

- Wybrane zagadnienia bezpieczeństwa warstwy sieciowej

- Bezpieczeństwo sieci WiFi

- Bezpieczeństwo aplikacji www

- Wybrane problemy bezpieczeństwa w architekturze sieci

- Bezpieczeństwo infrastruktury mobilnej (telefony, tablety)
- Bezpieczeństwo systemów operacyjnych oraz elementów oprogramowania infrastruktury
- Bezpieczeństwo IoT
- Elementy bezpieczeństwa informacji
- Testy penetracyjne – jako metoda testowania bezpieczeństwa sieci
- Modyfikacja komunikacji sieciowej
- Bezpieczeństwo sieci – Ethernet
- Bezpieczeństwo warstwy 3 modelu OSI
- Firewalle
- Bezpieczeństwo IPsec
- Bezpieczeństwo protokołów routingu
- Bezpieczeństwo web
- Systemy klasy IPS (Intrusion Prevention System) oraz firewalle aplikacyjne
- Podatności klasy buffer overflow
- Realizacja przykładowego testu penetracyjnego w LAB.