**Załącznik nr 5 do SWZ – część 1**

Opis przedmiotu zamówienia

Na potrzeby postępowania o udzielenie zamówienia publicznego

pn. **„Cyberbezpieczny Urząd Gminy Bukowiec”**

w zakresie:

* **części pierwszej: przeprowadzenie audytu obowiązkowego (końcowego) w pełnym zakresie KRI, przeprowadzenie cyklu szkoleń z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego oraz szkolenia dla pracownika IT z obecnych i dostarczonych rozwiązań.**

1. **Audyt obowiązkowy (końcowy) w pełnym zakresie KRI:**
2. Celem zamówienia jest weryfikacja zgodności funkcjonowania systemów teleinformatycznych w Urzędzie Miejskim w Mogilnie z przepisami rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności oraz wsparcie merytoryczne poaudytowe w celu dostosowania Urzędu do wymagań KRI.
3. Audyt powinien obejmować m. in.:
4. weryfikację zgodności z wymaganiami KRI w zakresie: bezpieczeństwa informacji, interoperacyjności, wymagań dotyczących struktur i formatów danych, zasad udostępniania informacji w systemach teleinformatycznych;
5. ocenę zgodności Polityki Bezpieczeństwa Informacji oraz dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji z wymaganiami KRI;
6. przegląd zabezpieczeń systemów IT;
7. analizę poziomu świadomości pracowników w zakresie bezpieczeństwa informacji;
8. wskazanie niezgodności i rekomendacji naprawczych.
9. W wyniku audytu wykonawca powinien dostarczyć **raport z audytu zgodności z KRI**, wykaz stwierdzonych niezgodności i zagrożeń, zalecenia i rekomendacje naprawcze, w razie potrzeby plan działań naprawczych.
10. Audyt musi być przeprowadzony zgodnie z:
11. wymogami 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. z 2024 r. poz. 773);
12. wytycznymi Ministerstwa Cyfryzacji dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych;
13. standardami informatycznymi RFC (zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum, związanych z Internetem oraz sieciami komputerowymi);
14. kodeksem „dobrych praktyk z dziedziny informatyki”, wskazówki CERT Polska czy też CSiRT;
15. stosownymi normami ISO (w tym ISO 27001, ISO 27002, ISO 27005/31000, ISO 24762, ISO 22301, itd.)
16. Opis środowiska Zamawiającego:
17. adres zamawiającego: ul. Dr Fl. Ceynowy 14, 86-122 Bukowiec i jest to jedyna lokalizacja urzędu;
18. liczba użytkowników: 28 osób;
19. dane dotyczące ilości komputerów, serwerów oraz innych urządzeń podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe, takie jak drukarki, routery, przełączniki, urządzenia VoIP itp.):
20. ilość komputerów: 29 szt.
21. ilość serwerów (fizycznych): 2
22. ilość pozostałych urządzeń:

* centrala telefoniczna – 1 szt.
* drukarki – 20 szt.
* UTM (urządzenie brzegowe) – 1 szt.

1. Forma audytu - audyt stacjonarny.
2. **Cykl szkoleń z zakresu cyberbezpieczeństwa dla pracowników Zamawiającego:**

1. Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa.

Szkolenia muszą być zrealizowane w siedzibie Zamawiającego.

W ramach szkolenia, uczestnicy muszą otrzymać konkretne porady do zastosowania w praktyce, tak aby możliwe było ich sprawne i zarazem bezpieczne funkcjonowanie w cyberprzestrzeni. Program kursu musi skupiać się na najważniejszych w danym obszarze aspektach. Trenerzy muszą zapewnić wysoki poziom merytoryczny oraz komunikacyjny.

Szkolenie ma zapoznać uczestnika z zagrożeniami, technikami ataków cyberprzestępczych oraz metodami socjotechnicznymi, ukierunkowanymi na osoby pracujące na co dzień przed komputerem.

Uczestnicy mają dowiedzieć się jak działa rynek cyberprzestępczy, jakimi kwotami operują współcześni przestępcy, jakimi sposobami próbują uzyskać dostęp do sieci teleinformatycznej oraz jak w czasie rozmowy osobistej, telefonicznej lub mailowej oszuści potrafią wyłudzić informację od nieświadomego pracownika. Podczas szkolenia uczestnik ma być również edukowany ze skutków, dla których wykorzystywanie komputera służbowego do celów prywatnych zwiększa ryzyko ataku na całą organizację.

Szkolenie musi być skierowane do każdego pracownika w organizacji bez względu na jego wiedzę i umiejętności informatyczne.

Korzyści po szkoleniu:

• zdobycie wiedzy obejmującej bezpieczne zarządzanie miejscem pracy oraz danymi

• zdobycie wiedzy umożliwiającej ochronę przed atakami socjotechnicznymi

Wykonawca zobowiązany jest do:

• wydania imiennych zaświadczeń / certyfikatów dla każdego uczestnika,

• zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

Szczegółowy wykaz szkoleń:

1) podstawy cyberbezpieczeństwa dla pracowników, o następującej tematyce:

• Wstęp do cyberbezpieczeństwa

• W jakim czasie następuje pierwszy atak?

• Po co ktoś ma nas atakować?

• Czy cyberprzestępczość się opłaca?

• Dane z raportów dotyczących stanu cyberbezpieczeństwa

• Aktualne zagrożenia związane z konfliktem na Ukrainie

• Rodzaje ataków cybernetycznych

• Co sprzyja atakom?

• Fałszywe bramki płatności

• Przykłady ataków ukierunkowanych na konkretną organizację

• Spoofing telefoniczny

• Sztuczna inteligencja, a cyberbezpieczeństwo

• Ataki na osoby fizyczne - co zrobić kiedy staniemy się ofiarą?

• Zasady postępowania z danymi uwierzytelniającymi

• Fałszywe strony, jako reklamy Google

• Ataki z wykorzystaniem kodów QR

• Największe wycieki danych w Polsce

• Ataki na systemy OT

• Sztuczki cyberprzestepców

• Podstawy ataków socjotechnicznych

• Jak bronić się przed socjotechniką?

• Zasady higieny w cyberprzestrzeni

1. **Szkolenia dla pracownika IT z obecnych i dostarczonych rozwiązań**

Zamawiający wymaga dostarczenia dwóch voucherów na szkolenia on-line, które zostaną zrealizowane przez certyfikowaną jednostkę szkoleniową, zapewniającą odpowiednią jakość i zgodność z obowiązującymi standardami.

1. MS-55371 Windows Server Administration

5-dniowy kurs prowadzony przez instruktora, stworzony dla pracowników sektora IT, którzy szukają doświadczenia w zarządzaniu Windows Server. Szkolenie przeznaczone dla osób odpowiedzialnych za zarządzanie tożsamością, zasobami, siecią i obliczanie za pomocą Windows Server. Podczas szkolenia, uczestnik pozna różne scenariusze, wymagania i opcje dostępne w Windows Server i dowie się jak je poprawnie zastosować w organizacji.

Po ukończeniu szkolenia, uczestnik będzie umiał:

- Używać technik i narzędzi do administracji Windows Server Wdrażać usługi tożsamości

- Zarządzać infrastrukturą sieci Konfigurować serwery plików i jego zasoby

- Zarządzać maszynami wirtualnymi przy użyciu wirtualizacji Hyper-V i kontenerów

- Zarządzać systemem wysokiej niezawodności i rozwiązaniami odnowy

- Stosować funkcje bezpieczeństwa w celu zabezpieczenia krytycznych danych

- Konfigurować usługi zdalnego centrum pomocy technicznej Konfigurować wdrażanie infrastruktury pulpitu bazując na maszynach wirtualnych

- Wdrażać zdalny dostęp i usługi sieciowe

- Wdrażać monitorowanie usług i wydajności, oraz rozwiązywać powiązane problemy

- Wprowadzać aktualizacje i migracje związane z AD DS. i zasobami

2. FortiGate - kompleksowa ochrona każdej sieci I (CCE-FGI)

Zdobycie umiejętności samodzielnej konfiguracji poszczególnych modułów bezpieczeństwa takich, jak: AntyVirus, AntySpam, WebFilter, IPS. Poznanie funkcjonalności modułu umożliwiającego kontrolę aplikacji. Zaprezentowanie dostępnych rozwiązań VPN.

Szkolenie przeprowadzane w formie warsztatów ze znaczną liczbą praktycznych laboratoriów. Zakres tematyczny oraz część warsztatowa dostosowana zostanie do potrzeb uczestników szkolenia.

Szkolenie oparte jest o FortiOS w wersji 7.x.