Załącznik nr 1

Opis wymagań

na:

przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa

dla kadry kierowniczej, pracowników nietechnicznych Urzędu Miejskiego w Jaworznie

1. Wstęp

Zamówienie jest realizowane w ramach grantu **„Cyberbezpieczny Samorząd”** współfinansowanego przez Unię Europejską z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (FERC) Priorytet II: *Zaawansowane usługi cyfrowe*, Działanie 2.2. – *Wzmocnienie krajowego systemu cyberbezpieczeństwa*, na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0346/FERC.02.02-CS.01-001/23/2024 z dnia 8 maja 2024 roku, projekt pn. „Wzmocnienie bezpieczeństwa teleinformatycznego w Gminie Miasta Jaworzna”.

W ramach projektu przewidziano:

- przygotowanie planu szkoleniowego dla pracowników nietechnicznych oraz kadry zarządzającej,
- przygotowanie materiałów szkoleniowych oraz udostępnienie platformy szkoleniowej dla pracowników Urzędu Miejskiego w Jaworznie (zwanych w dalszej części opracowania „Urzędem”),
- przeprowadzenie podstawowych szkoleń budujących świadomość cyberzagrożeń i sposobów ochrony przed nimi dla pracowników nietechnicznych Urzędu (przeszkolenie 500 pracowników) w celu zapewnienia regularnego podnoszenia poziomu cyberbezpieczeństwa.
- przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry zarządzającej Urzędu (przeszkolenie grupy maksymalnie 10 pracowników)
- dostarczenie voucherów na szkolenia z zakresu bezpieczeństwa teleinformatycznego on-line dla informatyków.

2. Wymagania ogólne (do wszystkich części zamówienia)

We wszystkich częściach zamówienia muszą zostać zachowane zasady równości szans i niedyskryminacji, w tym dostępność dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn. W przypadku szkoleń online, e-learningu (dostęp do platformy szkoleniowej) wymagane będzie spełnienie przez wykonawcę wymogów dostępności oraz WCAG 2.1 dla narzędzi/platform które zostaną wykorzystane do szkoleń. W ramach grup szkoleniowych przewidziana jest równa dostępność dla kobiet i mężczyzn oraz osób niepełnosprawnych. Opracowane dokumentacje będą musiały być dostarczone w formie elektronicznej z możliwością powiększania treści.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Wykonawca każdej z części zamówienia będzie zobowiązany do podpisania oświadczenia potwierdzającego przestrzeganie powyższych zasad.

3. Ogólny opis przedmiotu zamówienia

Przedmiotem zamówienia jest przeprowadzenie szkoleń z zakresu cyberbezpieczeństwa dla kadry kierowniczej oraz pracowników Urzędu. Zamówienie obejmuje:

- przeprowadzenie **podstawowych szkoleń** z zakresu cyberbezpieczeństwa w formie on-line z prowadzącym wraz z opracowaniem materiałów szkoleniowych,
- **dostarczenie i uruchomienie platformy szkoleniowej** do Urzędu (rozwiązanie może być oparte o rozwiązania Open Source), na której pracownicy będą mogli na bieżąco szkolić się z zakresu cyberbezpieczeństwa – platforma będzie wykorzystana do przeprowadzenia wśród pracowników Urzędu kursów rozszerzonych,
- **opracowanie i udostępnienie materiałów szkoleniowych (kurs rozszerzony)** na dostarczonej platformie szkoleniowej wraz z przekazaniem licencji dla Urzędu celem dalszego korzystania z dostarczonych materiałów z możliwością wykorzystania ich do szkolenia pracowników Urzędu oraz z prawem do modyfikacji treści przekazanych materiałów;
- **przeprowadzenie testów socjotechnicznych** (pierwszy test przed rozpoczęciem szkoleń i drugi po zakończonych szkoleniach, każdy na grupie min. 30 osób), pozwalających sprawdzić skuteczność szkoleń i zwrócić uwagę na kwestie wymagające dodatkowych szkoleń;
- **dostarczenie voucherów na szkolenia z zakresu bezpieczeństwa teleinformatycznego on-line dla informatyków do wykorzystania w 2025 roku.**

4. Szczegółowy opis przedmiotu zamówienia

Przedmiot zamówienia jest podzielony na 4 części. Ocena ofert zostanie przeprowadzona dla wszystkich części razem. Wykonawcy mogą składać oferty tylko na całość zamówienia.

4.1 Szkolenia podstawowe on-line z prowadzącym muszą spełniać następujące wymagania:

1. Szkolenia obejmują pracowników Urzędu.
2. Szkolenia muszą odbywać się w godzinach pracy Urzędu.
3. Wykonawca w ramach wykonania usługi przedstawi szczegółowy program szkolenia zawierający informacje dotyczące tematyki i czasu szkolenia oraz opracowane materiały i dostarczy je w terminie nie później niż 7 dni roboczych przed dniem rozpoczęcia szkolenia do akceptacji przez Zamawiającego.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

4. Opracowane materiały do szkolenia on-line będą musiały być dostarczone w formie elektronicznej z możliwością powiększania treści. W ramach wynagrodzenia Wykonawca przygotuje i zapewni materiały szkoleniowe dla każdego uczestnika, pozwalające na samodzielną edukację z zakresu tematyki szkolenia. Zamawiający wymaga dostarczenia kompletu materiałów do szkolenia on-line w formie elektronicznej, np. dokumenty w standardzie PDF.
5. Wykonawca dostarczy materiały szkoleniowe uczestnikom szkolenia najpóźniej w dniu rozpoczęcia szkolenia.
6. W ramach wynagrodzenia Wykonawca dostarczy Zamawiającemu materiały ze szkolenia, które to będzie mógł wykorzystać do przeszkolenia osób nieobecnych lub nowoprzyjętych w późniejszym okresie.
7. Każdy uczestnik szkolenia otrzyma od Wykonawcy imienny certyfikat z podpisem trenera, potwierdzający ukończenie szkolenia i jego zakres. Certyfikaty mogą być wydane w formie elektronicznej z wykorzystaniem podpisu elektronicznego.
8. Zamawiający zwraca uwagę, że szkolenia będące przedmiotem zamówienia mają charakter kształcenia zawodowego i są finansowane w całości ze środków publicznych, w związku z czym są one zwolnione z podatku od towarów i usług na podstawie §3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 roku w sprawie zwolnień od podatku towarów i usług oraz warunków stosowania tych zwolnień (t.j. Dz.U. 2023 poz. 955).

4.1.1 Szkolenia dla pracowników nietechnicznych

W ramach realizacji części 1. zamówienia Wykonawca zobowiązany będzie do przeprowadzenia **podstawowego szkolenia** on-line dla pracowników budującego świadomość cyberzagrożeń i sposobów ochrony dla pracowników JST. Celem szkolenia jest budowa świadomości i umiejętności praktycznych pracowników Urzędu w zakresie cyberzagrożeń i sposobów ochrony przed nimi oraz problematyki związanej z bezpieczeństwem informacji, w tym z codziennym zabezpieczaniem danych i reagowaniem na zagrożenia.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
2. cyberbezpieczeństwo w codziennej pracy urzędu,
3. standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

4. bezpieczeństwo urządzeń i bezpieczeństwo fizyczne, bezpieczne hasła, zarządzanie hasłami, uwierzytelnienie dwu- i wieloskładnikowe, klucze sprzętowe,
5. przegląd i rozpoznawanie najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa), sposoby unikania zagrożeń, zasady bezpiecznego korzystania z Internetu, Sztuczna Inteligencja.
6. ochrona informacji i prywatność w Internecie,
7. jak bezpiecznie korzystać z narzędzi teleinformatycznych w urzędzie – przykłady stosowania zabezpieczeń,
8. reagowanie na incydenty bezpieczeństwa (w tym zasady postępowania w razie podejrzenia naruszenia bezpieczeństwa/ataku),
9. procedury zgłaszania incydentów – ustalone z Zamawiającym – zgodne z obowiązującą u Zamawiającego Polityką Bezpieczeństwa Informacji.

Szkolenia mają obejmować ćwiczenia praktyczne (min. 25% czasu trwania szkolenia), pozwalające na podniesienie umiejętności związanych z:

- rozpoznawaniem zagrożeń i reagowanie na nie,
- wykorzystywaniem narzędzi informatycznych zapewniających bezpieczeństwo przetwarzanych informacji oraz zabezpieczeń i mechanizmów dla poczty elektronicznej i stron WWW,
- radzeniem sobie w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

W trakcie szkolenia trener musi odpowiadać na pytania uczestników. Dopuszczalne jest zorganizowanie sesji pytań i odpowiedzi na zakończenie szkolenia.

W efekcie odbytych szkoleń pracownicy mają być w stanie odróżnić typowe błędy techniczne od potencjalnego ataku, wiedzieć jak uniknąć potencjalnego zagrożenia, a w przypadku wystąpienia naruszenia – umieć podjąć podstawowe działania ograniczające skutki wystąpienia incydentu oraz zgłosić incydent do odpowiednich komórek.

Wymagana forma przeprowadzenia szkolenia: **szkolenie online z prowadzącym w grupach po 50 osób** plus dostęp do kursu rozszerzonego na platformie e-learningowej.

Liczba osób do przeszkolenia w ramach każdej edycji – 500 (min 10 grup, maksymalnie 50 osób w grupie).

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

Czas trwania szkolenia – min. 6 godzin lekcyjnych (po 45 min.).

Materiały użyte w trakcie szkolenia podstawowego on-line z prowadzącym pozostają do wykorzystania przez Urząd Miejski w Jaworznie do dalszych szkoleń dla pracowników Urzędu.

Z przeprowadzonych szkoleń Wykonawca musi przedstawić **listy obecności** (forma do uzgodnienia na etapie realizacji) z listą imienną uczestników szkolenia.

Szkolenie musi być zakończone **anonimową ankietą** wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu **podsumowanie wyników ankiety** oraz przekaże wszystkie ankiety Zamawiającemu.

Materiały edukacyjne przekazywane uczestnikom w formie PDF muszą posiadać loga projektu „Cyberbezpieczny Samorząd", oraz muszą zawierać informację o dofinansowaniu szkoleń z funduszy unii europejskiej.

4.1.2 Szkolenia dla Kadry Zarządzającej

W ramach realizacji tej części zamówienia, Wykonawca zobowiązany będzie do przeprowadzenia szkolenia specjalistycznego dla kadry kierowniczej w zakresie bezpieczeństwa informacji i wymogów w zakresie cyberbezpieczeństwa. Celem szkolenia jest zwiększenie świadomości kadry kierowniczej Urzędu w zakresie problematyki związanej z bezpieczeństwem informacji, rozwinięcie umiejętności strategicznego zarządzania cyberbezpieczeństwem oraz zrozumienie przepisów prawnych i ich implementacji.

Szkolenie musi obejmować co najmniej następującą tematykę:

1. podstawy cyberbezpieczeństwa (podstawowe pojęcia i zasady działania),
2. przegląd najpopularniejszych zagrożeń (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa),
3. znaczenie cyberbezpieczeństwa dla jednostki samorządu terytorialnego,
4. przegląd aktualnych zagrożeń i trendów w cyberprzestrzeni (w tym rodzaje ataków, ransomware i malware, phishing, oszustwa i wyłudzenia z uwzględnieniem oszustwa typu Business E-mail Compromise, atak telefoniczny, spoofing, atak odwrócony – zmuszenie ofiary do szukania pomocy u

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

atakującego, przekręt nigeryjski, wyłudzenia BLIK, oszustwo na dyrektora/prezesa), sposoby unikania zagrożeń, zasady bezpiecznego korzystania z Internetu, Sztuczna Inteligencja,

5. analiza przepisów 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) i ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2024 poz. 1077),
6. cyberbezpieczeństwo jednostki samorządu terytorialnego w kontekście bezpieczeństwa państwa,
7. zasady postępowania w razie wprowadzenia stopni alarmowych CRP dotyczących zagrożeń w cyberprzestrzeni,
8. obowiązki jednostek samorządu terytorialnego wynikające z przepisów,
9. metody identyfikacji i oceny ryzyka,
10. tworzenie i implementacja polityk ochrony danych,
11. standardy i najlepsze praktyki postępowania w celu zapewnienia cyberbezpieczeństwa w urzędzie, cyberhigiena,
12. procesy i procedury zarządzania incydentami oraz role poszczególnych pracowników,
13. rola kadry kierowniczej w zakresie cyberbezpieczeństwa (w tym w sytuacjach kryzysowych),
14. incydenty w kontekście zachowania ciągłości działania urzędu,
15. przywództwo, motywowanie zespołu i promocja kultury bezpieczeństwa w urzędzie.

Szkolenia mają obejmować ćwiczenia praktyczne (min. 25% czasu trwania szkolenia), pozwalające na podniesienie umiejętności związanych z:

- rozpoznawaniem zagrożeń i reagowanie na nie,
- analizą rzeczywistych incydentów (studia przypadków),
- zarządzaniem w sytuacjach kryzysowych (scenariusze codziennych zagrożeń).

W efekcie odbytych szkoleń kadra kierownicza musi być w stanie efektywnie zarządzać cyberbezpieczeństwem w urzędzie, podejmować strategiczne decyzje dotyczące ochrony danych oraz promować kulturę bezpieczeństwa wśród pracowników. Dzięki temu urząd będzie lepiej przygotowany na ewentualne zagrożenia i incydenty.

Wymagana forma przeprowadzenia szkolenia: **szkolenie online z prowadzącym w grupie do 10 osób** plus dostęp do kursu rozszerzonego na platformie e-learningowej.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Liczba osób do przeszkolenia w ramach każdej edycji – do 10 osób (1 grupa, maksymalnie 10 osób w grupie).

Czas trwania szkolenia – min. 6 godzin lekcyjnych (po 45 min.).

Materiały użyte w trakcie szkolenia podstawowego on-line z prowadzącym pozostają do wykorzystania przez Urząd Miejski w Jaworznie do dalszych szkoleń dla pracowników Urzędu.

Z przeprowadzonych szkoleń Wykonawca musi przedstawić **listy obecności** (forma do uzgodnienia na etapie realizacji) z listą imienną uczestników szkolenia.

Szkolenie musi być zakończone **anonimową ankietą** wśród uczestników, oceniającą co najmniej przydatność szkolenia, zakres przekazanych informacji, adekwatność przekazanych informacji do potrzeb uczestników, formę prezentacji i komunikatywność prowadzącego szkolenie. Wykonawca przedstawi Zamawiającemu **podsumowanie wyników ankiety** oraz przekaże wszystkie ankiety Zamawiającemu.

Materiały edukacyjne przekazywane uczestnikom w formie PDF muszą posiadać loga projektu „Cyberbezpieczny Samorząd", oraz muszą zawierać informację o dofinansowaniu szkoleń z funduszy unii europejskiej.

4.2 Dostarczenie i uruchomienie platformy szkoleniowej dla kursu rozszerzonego

Wykonawca dostarczy i uruchomi na infrastrukturze prowadzącego platformę do przeprowadzenia kursu rozszerzonego dla pracowników Urzędu. Dostarczona platforma nie może mieć ograniczeń czasowych użytkowania ani ilościowych co do użytkowników z niej korzystających oraz szkoleń jakie będą do niej wgrywane w trakcie niniejszego zamówienia jak i w późniejszym okresie. Dostarczone rozwiązanie może opierać się na oprogramowaniu Open Source (jest to rozwiązanie preferowane).

Dostarczone rozwiązanie musi umożliwiać:

- wprowadzanie na platformę kursów opracowanych przez Wykonawcę,
- wprowadzanie na platformę kursów opracowanych przez Zamawiającego w dowolnym zakresie czasowym,
- sprawdzanie nabytych umiejętności przez kursantów poprzez możliwość np. uruchomienia testów lub zadań do rozwiązania przez kursanta po zakończonej lekcji / kursie,
- dokonanie oceny kursantów,
- zarządzanie użytkownikami z możliwością tworzenia grup przypisanych do odpowiednich kursów,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

- umożliwiać podział co najmniej na 3 kategorie użytkowników : administrator platformy, administrator kursu, uczestnik kursu.

W przypadku gdy Wykonawca będzie posługiwać się platformą płatną musi dostarczyć licencję dla Urzędu Miejskiego w Jaworznie na nieograniczonych czas oraz liczbę użytkowników.

Dodatkowo platforma musi spełniać następujące wymagania:

1. działać w przeglądarkach internetowych (Microsoft Edge, Mozilla Firefox i Google Chrome), bez konieczności instalowania dodatkowych komponentów po stronie klienta,
2. posiadać interfejs użytkownika w języku polskim,
3. umożliwiać jednoznaczne zidentyfikowanie i uwierzytelnienie użytkownika za pomocą unikalnego loginu i hasła,
4. być dostosowana do potrzeb osób z niepełnosprawnościami zgodnie ze standardami WCAG 2.1 (w tym osobna wersja kontrastowa – przełączanie co najmniej na stronie startowej),
5. umożliwiać zalogowanemu użytkownikowi pełen dostęp do wszystkich udostępnionych przez administratora materiałów szkoleniowych i nieograniczony czas na zapoznanie się z materiałami szkoleniowymi przez cały czas dostępu do platformy,
6. materiały szkoleniowe muszą być podzielone na moduły w formie prezentacji multimedialnych, wzbogacone o filmy poglądowe z głosem lektora, animacje, itp.,
7. materiały muszą zawierać znacznik pokazujący w którym miejscu przerabianego materiału użytkownik się znajduje i ile kroków zostało do końca (liczbowo, np. slajd/strona 7 z 30, lub procentowo),
8. tekst wypowiadany przez lektora musi być również wyświetlony na ekranie na żądanie użytkownika,
9. umożliwiać sprawdzenie nabytej wiedzy za pomocą testów nieograniczonych czasem i liczbą podejść (dotyczy każdego z modułu szkoleniowych z osobna) – dla każdego testu określa się próg zaliczenia – ile % poprawnych odpowiedzi pozwala na zdanie testu,
10. testy muszą zawierać znacznik pokazujący w którym miejscu testu użytkownik się znajduje i ile kroków zostało do końca (liczbowo, np. pytanie 7 z 30, lub procentowo),
11. po zakończeniu testu użytkownik musi mieć możliwość sprawdzenia swoich odpowiedzi i porównania ich z poprawnymi – poprawne odpowiedzi powinny być opatrzone komentarzem wyjaśniającym dlaczego właśnie ta odpowiedź jest poprawna,
12. zapamiętywać dla każdego użytkownika postęp szkolenia poprzez oznaczenie materiałów jako przeglądane lub nie oraz rozpoczętych i zaliczonych testów,

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

13. posiadać panel administracyjny, w którym uprawniony użytkownik może przeglądać postępy indywidualne każdego z pozostałych użytkowników,

14. w panelu administracyjnym, uprawniony użytkownik może wygenerować raporty zbiorcze dla każdego użytkownika, każdego szkolenia, oraz dla wszystkich użytkowników wraz ze szczegółami dotyczącymi postępów i wyników testów.

4.3 Opracowanie i dostarczenie materiałów szkoleniowych dla kursu rozszerzonego

Wykonawca opracuje materiały szkoleniowe dla kursu rozszerzonego. Wykonawca opracowane materiały do kursu rozszerzonego dostarczy w terminie nie później niż 7 dni roboczych przed udostępnieniem ich na dostarczonej platformie, celem akceptacji treści przez Zamawiającego. Dla opracowanego materiału szkoleniowego zostaną opracowane testy weryfikujące wiedzę po przepracowaniu przez każdego uczestnika kursu poszczególnych grup tematycznych omawianych na kursie rozszerzonym. Wyniki testów muszą być dostępne dla administratorów kursu. Materiał do kursu rozszerzonego dla pracowników musi zawierać co najmniej następującą tematykę:

1. Bezpieczeństwo informacji – wprowadzenie.

Omówienie zagadnień: bezpieczeństwo informacji, zarządzanie bezpieczeństwem. Triada bezpieczeństwa: poufność, dostępność, integralność. Wprowadzenie do systemu zarządzania bezpieczeństwem informacji.

2. Phishing.

Czym jest phishing i jakie są jego odmiany? Przykłady ataków phishingowych – studium przypadków. Ochrona przed phishingiem. Jak rozpoznać próby wyłudzeń? Jak rozpoznać fałszywe wiadomości oraz witryny?

3. Internet - zasady bezpiecznego surfowania po stronach WWW.

Bezpieczne korzystanie z przeglądarek. Przykłady niepożądanych wtyczek i aplikacji webowych. Zasady i ograniczenia w dostępie do Internetu.

4. Portale społecznościowe – jak z nich korzystać?

Przykłady oszustw stosowane na portalach społecznościowych - studium przypadków. Wizerunek organizacji i własny w sieci – dlaczego należy zwracać uwagę na umieszczane tam informacje. Zasady świadomego korzystania z portali społecznościowych.

5. Poczta elektroniczna - zasady korzystania i ograniczenia.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

Firmowa poczta elektroniczna – zasady korzystania. Ograniczenia w korzystaniu z poczty elektronicznej. Pojęcie SPAM i podstawy prawne.

6. Jak zarządzać hasłami.

Idea kontroli dostępu: identyfikacja, uwierzytelnianie, autoryzacja. Obowiązki użytkowników mających dostęp do systemów teleinformatycznych. Zakazy i nakazy dotyczące tworzenia, zapisywania i zapamiętywania haseł. Ataki na hasła: online i offline. Menedżery haseł – zaszyfrowane sejfy.

7. Socjotechnika.

Scenariusze ataków socjotechnicznych – studium przypadków. Zasady ochrony przed atakami socjotechnicznymi.

8. Jak poprawnie zabezpieczyć sprzęt mobilny.

Możliwe reakcje w przypadku kradzieży i zagubienia sprzętu mobilnego.

Zasady bezpiecznej pracy na urządzeniach przenośnych wpływające na bezpieczeństwo danych.

9. Prawne aspekty i konsekwencje lekceważenia zasad bezpieczeństwa informacji.

Elementy Kodeksu Karnego odnoszące się do naruszenia i łamania zasad bezpieczeństwa informacji „Przestępstwa przeciwko ochronie informacji". Elementy Ustawy o Ochronie Danych Osobowych, o Prawach Autorskich i Prawach Pokrewnych. Wizerunek organizacji w sieci – aspekty prawne.

10. Stalking i cyberstalking.

10. Bezpieczeństwo płatności elektronicznych.

Jakie metody wykorzystują cyberprzestępcy, by zdobyć Twoje pieniądze. Na co zwracać uwagę przy korzystaniu z bankowości elektronicznej. Jakie przestępstwa wiążą się z płatnościami on-line i przy wykorzystaniu kart płatniczych.

11. Ransomware.

Ransomware i jak to wygląda w praktyce. Jakie są dobre praktyki w zakresie tworzenia kopii zapasowych danych. Rzeczywiste przykłady cyberataków na firmy i instytucje.

12. Zabezpieczenie fizyczne dokumentacji, sprzętu IT i pomieszczeń.

Ryzyka w zakresie braku zabezpieczenia dokumentacji przetwarzanej w organizacji, a także najlepsze sposoby jej zabezpieczania. Sposoby uzyskania nieautoryzowanego dostępu do komputerów oraz ryzyka związane z brakiem zabezpieczenia pomieszczeń, a także skutki z tym związane. Omówienie zagadnień na temat systemów wspomagających zabezpieczenia w warstwie fizycznej.

13. Wi-Fi.

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Moduł musi odnosić się do najnowszych zagrożeń ale też wyjaśniać cele, sposoby zabezpieczeń i ochrony sieci, bez których nie wyobrażamy już sobie teraz życia, a więc sieci bezprzewodowych.

14. Praca zdalna.

15. Vishing.

16. Fake newsy i dezinformacja.

17. Dane w Chmurze.

Rodzaje chmur obliczeniowych. Korzyści i zagrożenia związane z chmurami. Na co powinien zwracać uwagę pracownik - co robić, a czego się wystrzegać. Incydenty związane z przetwarzaniem danych w chmurze. Jak cyberprzestępcy wykorzystują chmurę.

4.4 Przeprowadzenie testów socjotechnicznych

Wykonawca przygotuje i przeprowadzi dwukrotnie testy socjotechniczne na pracownikach Urzędu Miejskiego w Jaworznie. Jeden test zostanie przeprowadzony przed rozpoczęciem szkoleń, drugi test zostanie przeprowadzony po zakończonych szkoleniach. Oba testy będą odbywać się na grupie co najmniej 30 osobowej. Wyniki testów będą przekazane w raporcie zbiorczym Zamawiającemu. Wykonawca będzie mógł korzystać z wyników testów w późniejszej jego działalności bez wskazywania jednostki oraz osób na których testy były realizowane jako studium przypadku.

4.5 Dostarczenie voucherów na szkolenia z zakresu bezpieczeństwa teleinformatycznego on-line dla informatyków.

Wykonawca w ramach umowy dostarczy następujące vouchery na szkolenia dla informatyków:

4.5.1 Szkolenie on-line Cyber Security Foundation dla 4 osób , Czas trwania: 24h dydaktyczne

Zakres szkolenia:

Podstawowe terminy stosowane w zarządzaniu cyberbezpieczeństwem

Zarządzanie ryzykiem, zgodnością (compliance)

Zapewnienie ciągłości działania i odtwarzanie po awarii

Zarządzanie bezpieczeństwem zasobów i danych

Bezpieczeństwo sieci i komunikacji

Zarządzanie tożsamością i użytkownikami

Kryptografia i PKI

Malware i bezpieczeństwo stacji końcowej (end-point security)

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | Centrum Projektów Polska Cyfrowa

Zarządzanie podatnościami (Vulnerability management)

Bezpieczeństwo fizyczne i regulacyjne

Polityki, procedury, standardy i rekomendacje bezpieczeństwa

Szkolenia i podnoszenie świadomości cyberbezpieczeństwa

Ataki i inżynieria socjalna (social engineering)

Bezpieczeństwo urządzeń mobilnych

4.5.2 Szkolenie on-line - SC 100T00 Microsoft Cybersecurity Architect dla 2 osób , Czas trwania 32 h dydaktyczne

Zakres szkolenia:

Moduł 1: Budowa ogólnej strategii i architektury bezpieczeństwa

Moduł 2: Projektowanie strategii operacji bezpieczeństwa

Moduł 3: Projektowanie strategii zabezpieczeń tożsamości

Moduł 4: Ocena strategii zgodności z przepisami

Moduł 5: Ocena stanu bezpieczeństwa i rekomendowanie strategii technicznych zarządzania ryzykiem

Moduł 6: Najlepsze praktyki w zakresie architektury i ich zmiany w chmurze

Moduł 7: Projektowanie strategii zabezpieczania punktów końcowych serwera i klienta

Moduł 8: Projektowanie strategii zabezpieczania usług PaaS, IaaS i SaaS

Moduł 9: Określanie wymagań bezpieczeństwa dla aplikacji

Moduł 10: Projektowanie strategii zabezpieczania danych

Moduł 11: Polecanie najlepszych rozwiązań w zakresie zabezpieczeń przy użyciu architektur referencyjnych cyberbezpieczeństwa firmy Microsoft (MCRA) i testów porównawczych zabezpieczeń chmury firmy Microsoft

Moduł 12: Polecanie bezpiecznej metodologii przy użyciu Cloud Adoption Framework (CAF)

Moduł 13: Polecanie strategii ransomware przy użyciu najlepszych praktyk zabezpieczeń firmy Microsoft

4.5.3 Szkolenie on-line - Linux – bezpieczeństwo systemu dla 2 osób , Czas trwania 24h dydaktyczne

Zakres szkolenia:

Różne rozumienie terminu ,,bezpieczeństwo'', np. kontrola dostępu czy spójność danych

Analiza ryzyka, kosztów i zysków związanych z bezpieczeństwem

Role administratorów i użytkowników

Bezpieczeństwo konsoli

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

• bezpieczeństwo konsoli fizycznej

• bezpieczeństwo konsoli zdalnej

Bezpieczeństwo systemów plików

• sprawdzanie spójności danych

• prawa i własność

• bezpieczne usuwanie plików

• szyfrowanie plików

• podpisywanie plików

• backup system

Techniki i infrastruktury uwierzytelniania

Zabezpieczanie kernela (SELinux,grsecurity)

Dzienniki systemowe

• zabezpieczanie plików dziennika

• zabezpieczanie przed fałszowaniem plików dziennika

• alternatywne systemy logowania

• monitorowanie plików dziennika

• login/ process accounting

Zabezpieczanie sieci

• omówienie zabezpieczania sieci pod kątem usług i protokołów

• zabezpieczanie dostępu przy użyciu narzędzia TCP Wrapper

• wykorzystanie SSL do zabezpieczania dostępu do usług sieciowych

• ochrona poczty elektronicznej

• detekcja ataków brute force

Główne założenia konfiguracyjne firewall'a

• omówienie właściwości i zadań firewall'a

• omówienie komponentów firewall'a

• omówienie zalet i wad różnych konfiguracji firewall'a.

• Konfiguracja firewalld

Omówienie filtrów pakietowych

• pojęcia filtracji pakietów

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA

- podstawy iptables, nftables
- zaawansowane własności iptables, nftables
- usługa NAT w systemie Linux.

Wirtualne Sieci Prywatne

- podstawowe własności VPN
- zaawansowana konfiguracja i nawiązywanie połączenia w usłudze IPSec
- zaawansowana konfiguracja i nawiązywanie połączenia w usłudze OpenVPN
- omówienie filtracji pakietów w sieci VPN

Wykrywanie włamań do sieci i metody reakcji na incydenty

- wykorzystanie logów systemowych i ich analiza
- wykrywanie włamań na poszczególnych maszynach (host intrusion)
- wykrywanie włamań z sieci (network intrusion)
- metody reakcji na incydenty

Fundusze Europejskie na Rozwój Cyfrowy | Rzeczpospolita Polska | Dofinansowane przez Unię Europejską | CENTRUM PROJEKTÓW POLSKA CYFROWA