

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Audyt końcowy w obszarze cyberbezpieczeństwa

Audyt powinien obejmować przynajmniej obszary, w których przetwarzane są dane osobowe wrażliwe, w tym kluczowe systemy informacji medycznej oraz infrastrukturę urządzeń medycznych (aparatura medyczna wraz z systemami je obsługującymi). Audyt powinien obejmować niezbędną infrastrukturę teleinformatyczną podmiotu, w tym przynajmniej bezpieczeństwo takich elementów jak:

- Kanały komunikacji jak np. poczta;
- Sieciowe urządzenia brzegowe wraz z zasadami segmentacji oraz przepływów;
- Kontrolery domeny;
- Platforma wirtualizacyjna;
- System zarządzania kopiami zapasowymi;
- Poprawność konfiguracji stacji roboczych oraz serwerów;
- Sposoby uwierzytelniania się użytkowników.

Zakres prac powinien obejmować:

- zrozumienie kontekstu działania organizacji w tym wpływ systemów IT i/lub OT na usługi;
- potwierdzenie realizacji obowiązków zgodnie z wymaganiami przepisów prawa;
- analizę dokumentacji dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usług;
- testy skuteczności funkcjonowania mechanizmów kontrolnych;
- opracowanie raportu zawierającego opis zidentyfikowanych niezgodności wraz z rekomendacjami;
- przedstawienie wyników audytu dla Najwyższego Kierownictwa.

Audyt powinien obejmować kompleksową ocenę następujących obszarów związanych z bezpieczeństwem informacji:

- Funkcjonowanie systemu zarządzania bezpieczeństwem informacji, w tym zgodność z przyjętymi standardami i procedurami;
- Aktualizowanie regulacji wewnętrznych dotyczących ochrony danych;
- Bieżącą inwentaryzację sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji;
- Regularne analizy ryzyka, oceniające zagrożenia związane z integralnością, dostępnością oraz poufnością informacji;
- Weryfikację uprawnień osób odpowiedzialnych za przetwarzanie informacji;
- Efektywność prowadzonych szkoleń dla pracowników zajmujących się przetwarzaniem informacji, pod kątem podnoszenia ich świadomości i kompetencji;
- Zastosowane środki ochrony przed kradzieżą danych, nieautoryzowanym dostępem, uszkodzeniami oraz innymi zagrożeniami, mające na celu zapewnienie odpowiedniego poziomu zabezpieczeń;
- Wdrożone zasady dotyczące bezpiecznej pracy zdalnej oraz przetwarzania mobilnego;

- Sposób zabezpieczenia informacji, uniemożliwiający jej nieuprawnione ujawnienie, modyfikację, usunięcie lub zniszczenie;
- Obowiązujące zapisy w umowach serwisowych zawartych ze stronami trzecimi, gwarantujące odpowiedni poziom bezpieczeństwa informacji;
- Procedury zarządzania informacjami, mające na celu ograniczenie ryzyka ich kradzieży lub nieautoryzowanego dostępu;
- Zastosowane mechanizmy ochrony w systemach teleinformatycznych, zapewniające odpowiedni poziom bezpieczeństwa operacyjnego;
- Procedury zgłaszania incydentów związanych z naruszeniem bezpieczeństwa informacji, umożliwiające szybkie reagowanie na zagrożenia;
- Regularne przeprowadzanie audytów wewnętrznych, weryfikujących skuteczność stosowanych rozwiązań w zakresie ochrony informacji.

W trakcie audytu konieczne jest dokonanie analizy aspektów związanych z bezpieczeństwem fizycznym, w tym środków ochrony dedykowanych pomieszczeniom, urządzeniom, infrastrukturze technicznej oraz personelowi, minimalizujące ryzyko wynikające z zagrożeń fizycznych, takich jak nieautoryzowany dostęp, kradzież czy inne incydenty. Dodatkowo, audyt powinien obejmować kwestie związane z bezpieczeństwem technologicznym, skoncentrowane na zabezpieczeniu systemów teleinformatycznych przed potencjalnymi zagrożeniami, oraz bezpieczeństwem organizacyjnym i osobowym, uwzględniającym procedury operacyjne, szkolenia pracowników oraz polityki ochrony danych.

Audyt musi zostać zrealizowany w siedzibie Zamawiającego i trwać co najmniej trzy dni robocze.

W ramach wykonania zadania audytorzy zobowiązani są do dostarczenia Zamawiającemu szczegółowego raportu podsumowującego przeprowadzone działania. Dokument ten powinien zawierać ocenę stanu cyberbezpieczeństwa oraz rekomendacje dotyczące jego poprawy, w tym wskazówki dotyczące wdrożenia dodatkowych zabezpieczeń, aktualizacji procedur lub optymalizacji rozwiązań technologicznych.

Podczas realizacji audytu wykonawca powinien kierować się następującymi normami i przepisami prawnymi:

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Rozporządzenie 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;
- Rozporządzenie 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;
- 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) (Tekst mający znaczenie dla EOG)

Zespół audytujący: co najmniej trzech audytorów posiadających certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC

27001 wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.

2. Wdrożenie systemu zarządzania bezpieczeństwem informacji na podstawie NIS 2

Wykonawca jest zobowiązany do wdrożenia u Zamawiającego kompleksowego SZBI, obejmującego polityki, procedury, działania, role, kompetencje i procesy mające na celu zarządzanie ryzykiem związanym z bezpieczeństwem informacji. SZBI musi być dopasowany do realiów operacyjnych Zamawiającego oraz charakterystyki jego systemów IT i OT.

SZBI musi objąć również plany ciągłości działania systemów oraz proces szacowania ryzyka. W pierwszym kroku musi zostać wykonany audyt przedwdrożeniowy względem wymagań KRI, UoKSC, NIS2, aby precyzyjnie określić braki organizacyjne, kompetencyjne i techniczne oraz ustalić priorytety i harmonogram działań. Przeprowadzone musi zostać również szacowanie ryzyka (na podstawie ISO/IEC 27005), obejmujące inwentaryzację aktywów, identyfikację zagrożeń i podatności, ocenę prawdopodobieństwa i skutków oraz opracowanie planu postępowania z ryzykiem.

W ramach przygotowania dokumentacji SZBI Wykonawca zobowiązany jest do uwzględnienia aspektów związanych z bezpieczeństwem fizycznym, technologicznym, osobowym i organizacyjnym, takich jak:

- ochrona obiektów, sprzętu, infrastruktury technicznej oraz personelu przed zagrożeniami, takimi jak kradzież, sabotaż czy nieuprawniony dostęp;
- ochrona systemów teleinformatycznych przed atakami cybernetycznymi, nieautoryzowanymi zmianami, awariami oraz błędami ludzkimi;
- ochrona informacji przed zagrożeniami osobowymi obejmującymi pracowników Zamawiającego oraz personel dostawców/partnerów.

SZBI musi obejmować minimum następujące obszary:

1. ustanowienie polityki bezpieczeństwa informacji oraz polityk tematycznych, w tym polityk analizy ryzyka i bezpieczeństwa systemów informatycznych;
2. aktualizacje regulacji wewnętrznych w zakresie bezpieczeństwa informacji;
3. utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji;
4. opracowanie polityk i procedur służących ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
5. przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji;
6. bezpieczeństwo zasobów ludzkich, polityka kontroli dostępu i zarządzanie aktywami;
7. podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia;
8. zapewnienie szkoleń osób zaangażowanych w proces przetwarzania informacji, w tym przeprowadzanie szkoleń w zakresie cyberbezpieczeństwa;
9. zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami;

10. ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
11. zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionym osobom jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
12. opracowanie polityk i procedur stosowania kryptografii;
13. bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między Zamawiającym, a jego bezpośrednimi dostawcami, usługodawcami i poddostawcami;
14. zawierania w umowach serwisowych, podpisanych ze stronami trzecimi, zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
15. ciągłość działania kluczowych usług, w tym zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej oraz zarządzanie kryzysowe;
16. stosowanie uwierzytelniania wieloskładnikowego oraz ciągłych, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych;
17. zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, w tym bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych oraz postępowanie w przypadku wykrycia podatności i ich ujawnianie;
18. zarządzanie incydentami bezpieczeństwa informacji i cyberbezpieczeństwa;
19. zapewnienia okresowego audytu w zakresie bezpieczeństwa informacji i cyberbezpieczeństwa;

Dokumentacja musi uwzględniać wymagania następujących aktów prawnych oraz norm:

- Ustawa o Krajowym Systemie Cyberbezpieczeństwa;
- Norma PN-EN ISO/IEC 27001:2023;
- Norma PN-EN ISO/IEC 27002:2023;
- Rozporządzenie 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;
- Rozporządzenie 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;
- 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) (Tekst mający znaczenie dla EOG)

Wykonawca ma obowiązek przekazać Zamawiającemu:

- pełną dokumentację systemu zarządzania bezpieczeństwem informacji;
- zalecenia mające na celu zwiększenie poziomu bezpieczeństwa informacji Zamawiającego.

3. Szkolenia związane z wdrożeniem oraz stosowaniem systemu zarządzania bezpieczeństwem informacji

W ramach realizacji usługi Wykonawca przeprowadzi szkolenia dla zespołu ds. SZBI, powołanego przez Zamawiającego, w którym omówione zostaną zasady funkcjonowania i utrzymania systemu zarządzania bezpieczeństwem informacji (SZBI).

Szkolenie z wdrażania udokumentowanego Systemu Zarządzania Bezpieczeństwem Informacji przygotowuje do zarządzania bezpieczeństwem w oparciu o normę ISO 27001, obejmując analizę kontekstu organizacji, szacowanie ryzyka, wybór i wdrażanie zabezpieczeń, tworzenie dokumentacji (polityk, procedur, instrukcji), a także audytowanie i ciągłe doskonalenie systemu w celu ochrony informacji przed zagrożeniami, zgodnie z wymaganiami prawnymi.

Główne cele szkolenia:

- Zrozumienie wymagań normy ISO/IEC 27001 - dogłębna analiza punktów normy, terminologii, celów bezpieczeństwa informacji, zasad przywództwa, planowania i funkcjonowania SZBI;
- Praktyczne umiejętności - nauka identyfikacji aktywów informacyjnych, analizy i oceny ryzyka (np. metodą PDCA), projektowania i wdrażania zabezpieczeń;
- Tworzenie dokumentacji - ćwiczenia z tworzenia polityki bezpieczeństwa, procedur, instrukcji i deklaracji stosowania.
- Rola pełnomocnika ds. SZBI oraz audytora wewnętrznego - wyjaśnienie roli koordynatora lub pełnomocnika SZBI, a także audytorów wewnętrznych.
- Aspekty prawne i organizacyjne - uwzględnienie wymagań prawnych (np. dyrektywy NIS 2), kontekstu organizacji, oczekiwań interesariuszy oraz roli zasobów ludzkich.

Minimalny program szkolenia:

- Wprowadzenie - definicje, zakres SZBI, rola dokumentacji (polityki, procedury);
- Kontekst organizacji - analiza otoczenia, identyfikacja interesariuszy;
- Przywództwo - wymagania dla kierownictwa;
- Planowanie - ustalanie celów, podejście oparte na ryzyku;
- Wsparcie - zasoby, kompetencje, komunikacja, dokumentacja;
- Funkcjonowanie - realizacja procesów, identyfikacja i ocena ryzyka;
- Ocena wyników - monitorowanie, pomiary, audyty wewnętrzne;
- Doskonalenie - działania korygujące i zapobiegawcze.
- Zabezpieczenia organizacyjne, osobowe, fizyczne i technologiczne
- Ćwiczenia praktyczne - identyfikacja ryzyka, tworzenie i przegląd dokumentów.

Wymiar szkolenia: co najmniej 4 godziny zegarowe na turę.

4. Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)

Szkolenia muszą być zrealizowane w siedzibie Zamawiającego.

Szkolenia pracowników administracji i pracowników medycznych, muszą obejmować co najmniej tematykę:

- Podstawowych zasad cyberhigieny;
- Typów ataków wraz z przykładami;
- Reagowania na incydenty;
- Odpowiedzialności prawnej.

Szkolenia kadry kierowniczej, muszą obejmować co najmniej tematykę:

- Podstaw prawnych w obszarze cyberbezpieczeństwa;
- Typów ataków wraz z przykładami;
- Reagowania na incydenty;
- Wykonywania testów bezpieczeństwa;
- Roli kadry zarządzającej w procesach bezpieczeństwa.

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 certyfikatów dla każdego uczestnika,
- zapewnienia dla każdego uczestnika materiałów szkoleniowych w formie elektronicznej.

Wymiar szkolenia: 2 godziny na turę.

Szczegółowa tematyka szkolenia dla pracowników:

- Wprowadzenie do bezpieczeństwa informacji
- Atrakcyjność ofiar
- Czy cyberprzestępczość się opłaca?
- Aktualne trendy w zakresie cyberbezpieczeństwa
- Aktualne zagrożenia związane z sytuacją geopolityczną
- Rodzaje ataków cybernetycznych
- Analiza faz ataków
- Oszustwa płatnicze

- Przykłady ataków ukierunkowanych na szpitale
- Spoofing telefoniczny i sms-owy
- Sztuczna inteligencja, a cyberbezpieczeństwo
- Jak postępować kiedy staniemy się ofiarą?
- Zasady postępowania z danymi uwierzytelniającymi
- Fałszywe strony WWW
- Ataki z wykorzystaniem kodów QR
- Największe wycieki danych w Polsce
- Ataki na systemy przemysłowe
- Sztuczki cyberprzestępców
- Podstawy ataków socjotechnicznych
- Jak bronić się przed socjotechniką?
- Zasady higieny w cyberprzestrzeni
- Aspekty bezpieczeństwa fizycznego

Szczegółowa tematyka szkolenia dla kierownictwa:

- Wstęp do bezpieczeństwa informacji;
- Akty prawne powiązane z bezpieczeństwem informacji;
- Krajowy System Cyberbezpieczeństwa;
- Analiza ataków cybernetycznych;
- Najpopularniejsze zagrożenia;
- Przewodnik po metodach obrony szpitala;
- Odpowiedzialność i zadania kierownictwa w kontekście NIS 2;
- Przywództwo w rozumieniu ISO 27001;
- Zasady ochrony danych osobowych;
- Ciągłość działania systemów szpitala;
- Cyberbezpieczeństwo osobiste;
- Postępowanie w pracy;
- ABC higieny pracy w cyberprzestrzeni;
- Bezpieczeństwo pracy zdalnej;
- Ataki socjotechniczne;
- Ataki DoS/DdoS;
- Aktualne zagrożenia wynikające z wojny w Ukrainie.

5. Usługa testowania bezpieczeństwa (skany podatności)

Usługa testowania bezpieczeństwa obejmuje automatyczne skanowanie podatności testowanego środowiska, przeprowadzona zgodnie z założeniem że zespół testujący przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności.

Celem przeprowadzenia testów podatności systemu teleinformatycznego ma być zidentyfikowanie słabych punktów bezpieczeństwa, opierając się na zidentyfikowanych podatnościach.

Testy muszą obejmować hosty w sieci wewnętrznej oraz dostępne z poziomu sieci publicznej w wyznaczonych adresacjach.

Dodatkowo wykonawca musi przeprowadzić analizę topologii sieci wraz z próbami wykrycia nieszczelności w skonfigurowanych urządzeniach.

Testy muszą składać się z następujących faz:

- Faza rozpoznania - rozpoznanie aktywne obejmuje działania mające na celu zebranie informacji o testowanym systemie. Aktywność testującego opiera się na bezpośredniej interakcji ze środowiskiem celu. Zawiera w sobie działania takie jak skanowanie portów, wykrywanie usług czy hostów działających w sieci.
- Faza oceny podatności sieci wewnętrznej oraz urządzeń dostępnych z poziomu sieci internet: analiza występowania w badanym systemie podatności zawartych w bazach danych podatności, ocena wykorzystania skompromitowanych protokołów, weryfikacja słabości systemu na popularne ataki, próby eksploatacji wykrytych podatności technicznych,
- przygotowanie raportu z oceny wraz z zaleceniami działań naprawczych.

Testy muszą być przeprowadzone przez aktualne narzędzia wykorzystujące najnowsze bazy podatności.

Zakres testów:

- testy bezpieczeństwa sieci teleinformatycznych w tym brzegu sieci,
- testy bezpieczeństwa baz danych,
- testy bezpieczeństwa środowisk serwerowych w tym systemów operacyjnych,
- testy bezpieczeństwa środowisk wirtualnych,
- Konsultacje z zamawiającym.

Wykonawca zobowiązany jest do

- wykrycia działających usług w systemie teleinformatycznym,
- wykrycia otwartych portów na poszczególnych urządzeniach,
- zidentyfikowania podatności na poszczególnych hostach,
- wyszukania błędów konfiguracyjnych,
- określenia stopnia istotności wykrytych podatności technicznych,
- opracowania raportu podsumowującego z zaleceniami działań naprawczych.

6. Usługa testów socjotechnicznych wobec pracowników

Przeprowadzenie kampanii phishingowej oraz przygotowanie raportu zawierającego wyniki z analizą kampanii.

- wybór domeny (ładząco podobnej do prawdziwych domen Zamawiającego), która zostanie wykorzystana do kampanii phishingowej;
- opracowanie bazy mailingowej pracowników objętych kampanią phishingową oraz spreparowanego dokumentu zbliżonego wyglądem do dokumentów Zamawiającego, zawierającego dodatkowy niezłośliwy kod pozwalający na mierzenie efektów kampanii;

- wyznaczenie osób wtajemniczonych w fakt przeprowadzania testów (np. najwyższe kierownictwo, dział informatyczny lub wyłącznie szef tego działu, inspektor ochrony danych lub inna osoba odpowiedzialna za bezpieczeństwo w organizacji);
- dodanie domeny wybranej do przeprowadzenia kampanii phishingowej do tzw. białej/zaufanej listy w celu pominięcia filtrów antyspamowych (celem testu jest dostarczenie spreparowanej wiadomości na wszystkie skrzynki pracowników i weryfikacja ich podatności na prawdziwe kampanie cyberprzestępców);
- przeprowadzenie kampanii phishingowej (wysyłanie przygotowanej uprzednio wiadomości e-mail do pracowników wskazanych w bazie mailingowej)
- raport z testu phishingowego

Testy muszą być zrealizowane w wymiarze co najmniej 7 dni roboczych (tj. 16 godzin).

Przeprowadzenie prób ataków socjotechnicznych polega na wywieraniu wpływu na ludzi i stosowaniu perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji.

Przeprowadzane próby w Organizacji miały na celu zweryfikowanie świadomości pracowników i zabezpieczeń przed atakami socjotechnicznymi.

Testy muszą składać się z następujących faz:

- Rozpoznanie (biały wywiad, obserwacja pracy pracowników).
- Budowanie więzi i zaufania (użycie wewnętrznych informacji, podawanie się za kogoś innego, wspominanie nazwisk osób znanych ofierze, zgłoszenie potrzeby pomocy lub zasugerowanie posiadania władzy).
- Wykorzystanie zaufania (prośba o informację lub działanie skierowana do ofiary).

Testy muszą być przeprowadzone za pomocą aktualnych narzędzi, wykorzystujących najnowsze możliwości w zakresie symulacji złośliwych kampanii socjotechnicznych.

Zakres testów:

- Ataki typu phishing,
- Ataki typu spear phishing
- Phishing typu whaling
- Phishing przez klonowanie
- Angler phishing

Wykonawca zobowiązany jest do wykrycia (w stosunku do konkretnego adresu email):

- otwieranych wiadomości,
- otwierania plików w popularnych formatach, takich jak „docx.”, czy „xlsx”.
- otwieranych stron za pomocą linków umieszczonych w wiadomościach,
- podawanych poświadczeń na stronach mających na celu wyłudzenie informacji, przygotowanych przez testerów.

7. Platforma e-learningowa ze szkoleniami z zakresu cyberbezpieczeństwa

Przedmiotem zamówienia jest nowoczesna platforma e-learningowa oferująca szkolenia z zakresu cyberbezpieczeństwa. Platforma powinna zapewniać podnoszenie kompetencji pracowników oraz umożliwiać efektywną naukę w dowolnym miejscu i czasie, przy zachowaniu najwyższych standardów edukacyjnych. Platforma powinna posiadać intuicyjny interfejs umożliwiający skuteczne i wygodne przyswajanie wiedzy.

Użytkownicy powinni móc wybierać kursy zgodnie ze swoimi potrzebami, tworząc indywidualne ścieżki rozwoju. Kursy muszą być wzbogacone o interaktywne elementy, takie jak quizy, zadania praktyczne, studia przypadków, które ułatwiają zrozumienie skomplikowanych zagadnień. Platforma musi być dostępna o każdej porze dnia i nocy, pozwalając na naukę w dogodnym dla użytkownika momencie, bez konieczności dostosowywania się do sztywnych harmonogramów. System musi pozwalać na śledzenie postępów w nauce, w tym osiągania kolejnych etapów szkolenia. Każdy kurs musi być zakończony testem wiedzy, a po jego zdaniu uczestnik musi otrzymać certyfikat potwierdzający zdobyte kompetencje. Użytkownicy powinni posiadać dostęp do wsparcia technicznego, a także do ekspertów, którzy mogą pomóc w rozwiązywaniu trudnych kwestii związanych z materiałem kursu. Kursy muszą być dostosowane do różnych poziomów zaawansowania i potrzeb użytkowników. Wykonawca musi zapewnić regularnie aktualizowane materiały szkoleniowe, zgodne z najnowszymi trendami i wytycznymi w zakresie cyberbezpieczeństwa.

Wymagania funkcjonalne

1. Szkolenia muszą być dostępne w języku polskim.
2. Osoby opracowujące materiał szkoleniowy muszą posiadać certyfikaty audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.
3. Uczestnicy szkoleń muszą mieć możliwość skorzystania ze wsparcia merytorycznego (dot. materiału szkoleniowego – np. wyjaśnienie poruszanej problematyki poszczególnych modułów kursu) specjalistów w zakresie cyberbezpieczeństwa, którzy posiadają certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydane przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338), w zakresie certyfikacji osób.
4. Platforma powinna umożliwiać zamieszczanie różnych aktywności takich jak testy, ankiety, filmy wideo, webinary, artykuły czy wszelkiego rodzaju dokumenty.
5. Platforma musi umożliwiać zapisy do kursów w sposób zautomatyzowany.
6. Platforma musi umożliwiać import użytkowników z pliku CSV.
7. Platforma musi umożliwiać dostęp do informacji o uczestnikach kursu, śledzenie ich aktywności oraz ocenianie zadań.
8. Platforma musi umożliwiać weryfikowanie przekazanej wiedzy w formie testów sprawdzających o ustalonych progach zdawalności oraz przy pomocy quizów z losowym wybieraniem pytań z puli.
9. System musi posiadać funkcjonalność tworzenia ankiet ewaluacyjnych, raportów ze szkoleń i ich składowych oraz eksportu ich wyników do arkuszy kalkulacyjnych.
10. Platforma musi zapewniać tworzenie raportów i statystyk, obejmujących co najmniej następujące dane:
 - aktywni użytkownicy, zapisy na kurs i wskaźnik ukończenia kursu,
 - postęp kursu,
 - popularne kursy,

- statystyki certyfikatów,
 - użytkownicy w czasie rzeczywistym,
 - informacje o dostępie do witryny,
 - codzienna aktywność,
 - lista nieaktywnych użytkowników,
 - raport zbiorczy.
11. Platforma powinna umożliwiać tworzenie certyfikatów i zaświadczeń zgodnych z identyfikacją wizualną Zamawiającego oraz udostępnianie ich użytkownikom po każdym ukończonym kursie.
 12. Platforma musi posiadać narzędzia komunikacyjne dla użytkowników w postaci co najmniej czatów, forum, tablicy ogłoszeń, komunikatów, powiadomień e-mail.

Wymagania bezpieczeństwa

1. Platforma musi być oparta o stale aktualizowany system do zarządzania nauką (LMS).
2. Platforma powinna posiadać certyfikat SSL – opłacony przez Wykonawcę.
3. Platforma musi przechowywać hasła użytkowników w postaci zaszyfrowanej.
4. Wykonawca musi zapewniać bieżące aktualizacje serwera, bazy danych i Platformy.
5. Wykonawca musi zapewnić automatyczne kopie zapasowe Platformy.
6. Wykonawca musi wykonywać systematyczne, okresowe testy bezpieczeństwa (nie rzadziej niż raz na kwartał oraz przy większych zmianach w wykorzystywanych technologiach) Platformy oraz infrastruktury teleinformatycznej, z której korzysta Platforma.
7. Serwery Platformy muszą znajdować się w data center, które spełnia najwyższe standardy bezpieczeństwa fizycznego i technologicznego. Obejmujące zaawansowane zabezpieczenia przeciwpożarowe, kontrolę dostępu oraz systemy redundantne, które zapewniają ciągłość działania Platformy.
8. Wszystkie dane przesyłane między użytkownikiem, a Platformą muszą być szyfrowane za pomocą protokołu SSL/TLS.
9. System zarządzania uprawnieniami musi pozwalać na precyzyjne określenie, jakie dane i funkcje są dostępne dla poszczególnych użytkowników.
10. Platforma musi działać zgodnie z przepisami RODO, zapewniając zgodność z wymaganiami dotyczącymi ochrony danych osobowych.

Minimalny zakres tematyczny szkoleń:

Szkolenia dla kadry kierowniczej:

- Podstawy prawnych w obszarze cyberbezpieczeństwa;
- Typy ataków;
- Reagowanie na incydenty;
- Wykonywanie badań bezpieczeństwa;
- Rola kadry zarządzającej w procesach bezpieczeństwa.

Szkolenia dla kadry biurowej i medycznej:

- Podstawowe zasady cyberhigieny;
- Typy ataków wraz z przykładami;
- Reagowanie na incydenty.

Wycena szczegółowa

Zakres rzeczowy	Ilość	Wartość netto	Wartość Vat	Wartość brutto
Audyt końcowy w obszarze cyberbezpieczeństwa	1			
Wdrożenie systemu zarządzania bezpieczeństwem informacji na podstawie NIS 2	1			
Szkolenia związane z wdrożeniem oraz stosowaniem systemu zarządzania bezpieczeństwem informacji	1			
Szkolenia z zakresu podnoszenia świadomości w obszarze cyberbezpieczeństwa (cyberhigieny)	1			
Usługa testowania bezpieczeństwa (skany podatności)	1			
Usługa testów socjotechnicznych wobec pracowników	1			
Platforma e-learningowa	1			
	RAZEM			