## Zadanie nr 1 - Audyt systemu bezpieczeństwa informacji - 1 jednostka.

I. ZAKRES PRAC

1. Przeprowadzenie:
   a. audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI, obejmującego środowisko teleinformatyczne (IT) oraz środowisko technologii operacyjnej (OT), w tym systemy sterowania i automatyki przemysłowej (ICS/SCADA, PLC, HMI, systemy BMS/BAS) wraz ze stykami sieci IT-OT,
   b. analizę efektywności działań w zakresie monitorowania, pomiarów, analizy i oceny SZBI, w tym przegląd wskaźników ryzyka i zgodności.
2. Audyt w obszarze organizacyjnym obejmuje dwa komponenty: audyt bezpieczeństwa oraz audyt zgodności z przepisami i normami. Każdy z komponentów realizowany jest odrębnie dla środowiska IT oraz dla środowiska OT, z uwzględnieniem różnic w wymaganiach dostępności, ciągłości procesu technologicznego i cyklu życia systemów. Audyt powinien obejmować:
   a. Analiza wstępna i określenie zakresu audytu
      - Zdefiniowanie obszarów, lokalizacji oraz jednostek organizacyjnych objętych SZBI.
      - Inwentaryzacja i rozgraniczenie środowiska IT oraz OT, w tym identyfikacja stref i kanałów komunikacyjnych (podział na strefy/conduits) oraz punktów styku obu środowisk.
      - Weryfikacja ewidencji obszaru przetwarzania informacji, w tym dokładność danych dotyczących lokalizacji, kondygnacji i adresów.
      - Sprawdzenie czy zakres SZBI jest zgodny z wymaganiami normy PN-EN ISO/IEC 27001:2023-08 oraz potrzebami organizacji.
   b. Weryfikacja dokumentacji systemowej
      - Wprowadzenie do SZBI: Ocena czy dokumentacja zawiera podstawowe zasady zarządzania bezpieczeństwem informacji i zgodność z cyklem PDCA (Plan-Do-Check-Act).
      - Terminy i definicje: Sprawdzenie, czy wszystkie istotne pojęcia są zdefiniowane i zgodne z normami.
      - Kontekst organizacji: Analiza czynników wewnętrznych i zewnętrznych oraz ich wpływu na SZBI, w tym analiza ryzyk.
   c. Zarządzanie ryzykiem
      - Ocena procesu identyfikacji i analizy ryzyk, w tym dokumentacji dotyczącej szacowania ryzyk.
      - Analiza działań zaradczych i korygujących dla zidentyfikowanych ryzyk.
      - Weryfikacja, czy w analizie ryzyka dla środowiska OT uwzględniono skutki dla ciągłości procesu technologicznego, bezpieczeństwa ludzi i środowiska, a priorytet atrybutów bezpieczeństwa (dostępność-integralność-poufność) został określony odrębnie niż dla IT.
   d. Zabezpieczenia i deklaracja stosowania
      - Weryfikacja czy deklaracja stosowania zabezpieczeń jest zgodna z Załącznikiem A normy PN-EN ISO/IEC 27001:2023-08.
      - Ocena skuteczności wdrożonych zabezpieczeń oraz uzasadnienia ewentualnych wyłączeń.

- Ocena zabezpieczeń środowiska OT w odniesieniu do wymagań serii norm PN-EN IEC 62443 (w szczególności 62443-2-1 oraz 62443-3-3), w tym segmentacji sieci, kontroli zdalnego dostępu, zarządzania podatnościami i aktualizacjami w systemach o ograniczonych oknach serwisowych.

e. Dokumentacja operacyjna
   - Polityki i procedury: Sprawdzenie polityk bezpieczeństwa (np. kryptografii, zarządzania dostępem, bezpieczeństwa zasobów ludzkich) i ich zgodności z wymaganiami normatywnymi.
   - Ewidencje i rejestry: Ocena kompletności i aktualności ewidencji aktywów, obszarów przetwarzania informacji oraz rejestrów incydentów i zgłoszeń.
   - Zarządzanie dostępem: Sprawdzenie procedur przyznawania, zmiany i odbierania dostępu oraz zgodności z dokumentacją.

f. Monitorowanie i doskonalenie SZBI
   - Ocena procesów monitorowania, analizy i oceny systemu w odniesieniu do zgodności z wymaganiami i celami bezpieczeństwa.
   - Weryfikacja raportów z monitorowania, przeglądów zarządzania i działań korygujących.
   - Analiza działań doskonalących, w tym ocena skuteczności realizowanych zmian.

g. Zarządzanie incydentami i ciągłością działania
   - Ocena polityki zarządzania incydentami, w tym procedur zgłaszania, oceny i reagowania na incydenty.
   - Sprawdzenie planów zarządzania ciągłością działania i odtwarzania po katastrofie, w tym testów i analiz RTO, RPO, MTPD i MBCO.
   - Weryfikacja scenariuszy reagowania i odtwarzania dla środowiska OT, w tym procedur awaryjnego przejścia w tryb pracy ręcznej, odtwarzania konfiguracji sterowników i stacji operatorskich oraz posiadania kopii zapasowych oprogramowania narzędziowego i projektów aplikacyjnych.

h. Audyty wewnętrzne
   - Weryfikacja programu i planów audytów wewnętrznych, w tym ocena zgodności z wymaganiami normy PN-EN ISO/IEC 27001:2023-08.
   - Sprawdzenie raportów z audytów wewnętrznych pod kątem ustaleń, zgodności i zaleceń.

i. Zgodność z przepisami i ochroną danych osobowych
   - Ocena dokumentacji dotyczącej przetwarzania danych osobowych, w tym zgodności z RODO.
   - Weryfikacja rejestrów czynności przetwarzania danych, ocen skutków dla ochrony danych oraz testów równowagi.

j. Dokumentacja operacyjna
   - Analiza polityk i procedur dotyczących korzystania z systemów, urządzeń i sieci.
   - Weryfikacja zasad postępowania z nośnikami informacji, tworzenia haseł i korzystania z Internetu oraz poczty elektronicznej.

k. Zarządzanie dostawcami

- Sprawdzenie polityk i procedur związanych z bezpieczeństwem informacji w relacjach z dostawcami.
- Ocena zgodności działań dostawców z wymaganiami organizacji.

l. Zgodność z przepisami i normami

- Weryfikacja dokumentacji dotyczącej monitorowania i przestrzegania wymagań prawnych, regulacyjnych i umownych.
- Analiza zgodności z politykami zgodności oraz wynikami audytów technicznych, wraz ze wskazaniem stopnia spełnienia wymagań.
- Ocena zgodności z przepisami powszechnie obowiązującymi, w tym z ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w brzmieniu nadanym ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. z 2026 r. poz. 252), wdrażającą dyrektywę (UE) 2022/2555 (NIS 2), ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2026 r. poz. 1241) wraz z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247) oraz rozporządzeniem (UE) 2016/679 (RODO).
- Ocena zgodności z normami: PN-EN ISO/IEC 27001:2023-08, PN-EN ISO/IEC 27002:2023-01, PN-EN ISO/IEC 27005:2025-01, PN-EN ISO 22301:2020-04 - dla środowiska IT, oraz PN-EN IEC 62443 (części 2-1, 2-4, 3-2, 3-3, 4-2) - dla środowiska OT. Oceny dokonuje się według wydań norm aktualnych na dzień rozpoczęcia audytu.
- Sporządzenie macierzy zgodności wskazującej dla każdego wymagania przepisu lub normy status spełnienia (spełnione / spełnione częściowo / niespełnione / nie dotyczy) wraz z uzasadnieniem i dowodem audytowym.

II. DO ZADAŃ WYKONAWCY BĘDZIE NALEŻEĆ

1. Przeprowadzenie szczegółowej analizy i oceny SZBI, obejmującej:
   a. Identyfikację niezgodności i słabości w dokumentacji oraz wdrożeniu systemu.
   b. Przeprowadzenie wywiadów z wybranym personelem, w tym Pełnomocnikiem ds. Bezpieczeństwa Informacji.
2. Przekazanie dla Kierownika/Dyrektora Jednostki oraz dla Zamawiającego podpisanego przez audytora raportu z audytu wdrożonego w Jednostce systemu bezpieczeństwa informacji SZBI zawierający:
   a. Ustalenia audytu: Identyfikacja mocnych stron, niezgodności oraz obszarów wymagających doskonalenia.
   b. Rekomendacje: Propozycje działań korygujących i doskonalących.
   c. Ocena zgodności z normami i przepisami: wskazanie poziomu zgodności SZBI z wymaganiami przepisów i norm, o których mowa w pkt I.2 lit. l, odrębnie dla środowiska IT i środowiska OT, w formie macierzy zgodności.
3. Wykonawca udokumentuje wykonanie zadania poprzez okazanie protokołu odbioru.

4. Dokumentowanie realizacji zadania poprzez:
   a. Sporządzenie protokołu odbioru audytu.
   b. Wskazanie osób odpowiedzialnych za wdrożenie działań pokontrolnych.

III. UPRAWNIENIA

1. Audyt systemu bezpieczeństwa informacji wdrożonego u Grantobiorcy zostanie przeprowadzony na wniosek Grantobiorcy przez audytora zewnętrznego posiadającego przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999):
   1. Certified Internal Auditor (CIA);
   2. Certified Information System Auditor (CISA);
   3. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN-EN ISO/IEC 27001 wydany 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. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN-EN ISO 22301 wydany przez jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, w zakresie certyfikacji osób;
   5. Certified Information Security Manager (CISM);
   6. Certified in Risk and Information Systems Control (CRISC);
   7. Certified in the Governance of Enterprise IT (CGEIT);
   8. Certified Information Systems Security Professional (CISSP);
   9. Systems Security Certified Practitioner (SSCP);
   10. Certified Reliability Professional;
   11. Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert
2. Zamawiający zastrzega możliwość weryfikacji uprawnień audytorów (ważności uprawnień, akredytacja jednostki wydającej uprawnienia).

Cyberbezpieczne Wodociągi

**Zadanie nr 2 - Audyt zgodności ze standardami ustawy o krajowym systemie cyberbezpieczeństwa - 1 sztuka.**

1. Ocena wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI)
   - Weryfikacja formalnego powołania SZBI w organizacji.
   - Analiza ról i odpowiedzialności związanych z cyberbezpieczeństwem.
   - Ocena poziomu dojrzałości procesów zarządzania bezpieczeństwem informacji.
2. Przegląd dokumentacji SZBI
   - Analiza polityki bezpieczeństwa informacji pod kątem zgodności z wymaganiami UoKSC, ISO/IEC 27001 i wytycznymi KRI.
   - Przegląd polityk i procedur.
   - Ocena kompletności rejestrów (aktywa, incydenty, ryzyka, uprawnienia użytkowników).
   - Weryfikacja aktualności dokumentacji (data zatwierdzenia, okresowe przeglądy, podpisy osób odpowiedzialnych).
3. Kontrola zgodności z wymogami UoKSC
   - Weryfikacja formalnego wyznaczenia podmiotu odpowiedzialnego za cyberbezpieczeństwo i zgłoszenia do CSIRT.
   - Sprawdzenie implementacji wymaganych środków ochrony (organizacyjnych, procesowych, technicznych).
   - Weryfikacja procedur i rzeczywistych działań związanych ze zgłaszaniem incydentów poważnych do właściwego CSIRT.
   - Ocena systemu monitorowania, detekcji i reakcji na zagrożenia (SIEM, IDS/IPS, SOC, narzędzia logowania).
4. Wywiady z kluczowym personelem
   - Rozmowy z zarządem / kierownictwem w zakresie świadomości strategicznej dotyczącej cyberbezpieczeństwa.
   - Ocena kompetencji i poziomu wyszkolenia zespołu ds. cyberbezpieczeństwa (szkolenia, certyfikaty, doświadczenie).
   - Badanie świadomości pracowników w zakresie polityk bezpieczeństwa i obowiązków związanych z cyberbezpieczeństwem.
5. Analiza techniczna systemów informatycznych
   - Przegląd architektury IT i mapy systemów wspierających usługi kluczowe.
   - Weryfikacja konfiguracji systemów bezpieczeństwa (zapory, antywirusy, EDR, systemy backupu).
   - Kontrola logów bezpieczeństwa i rejestrów zdarzeń pod kątem śladów naruszeń.
   - Analiza poprawności zarządzania dostępami i uprawnieniami użytkowników.
6. Identyfikacja niezgodności
   - Sporządzenie listy niezgodności w odniesieniu do UoKSC.
   - Klasyfikacja niezgodności
   - Analiza potencjalnych zagrożeń i ich wpływu na ciągłość działania organizacji.
   - Identyfikacja ryzyk związanych z łańcuchem dostaw i współpracą z podmiotami trzecimi.

7. Opracowanie raportu końcowego z rekomendacjami
   - Przygotowanie szczegółowego raportu z ustaleń audytu.
   - Rekomendacje dotyczące doskonalenia SZBI.

**Zadanie nr 3 - Testy penetracyjne - 1 usługa (czas trwania testów: 5 dni roboczych).**

Wykonawca posiada potencjał techniczny i osobowy niezbędny do wykonania zamówienia.
Potencjał techniczny przedstawia się poprzez posiadanie narzędzi takich jak automatyczny skaner podatności posiadający funkcje pozwalające na:

- wykonanie skanowań z wykorzystaniem wbudowanych szablonów;
- skanowanie sieciowe (wykrywanie otwartych portów i rozpoznanie uruchomionych na nich usług, wskazywanie listy podatności na wykryte usługi);
- weryfikacje domyślnych haseł według zadanego słownika;
- skanowanie systemów operacyjnych z uwierzytelnieniem (sprawdzenie wersji systemu, zainstalowanych na nim aplikacji, brakujących aktualizacji, wskazywanie listy podatności na wykryte systemy i aplikacje) oraz weryfikację uprawnień zadanego użytkownika;
- ustawienia harmonogramu skanowań;
- możliwość porównania wyników poszczególnych skanowań;
- możliwość konfigurowania zawartości raportu ze skanowania oraz dobieranie różnych formatów wyjściowych raportów (w tym HTML, CVS i XML);
- możliwość wyświetlania wyników na bieżąco oraz możliwość grupowania podobnej klasy podatności i możliwość sortowania po IP i podatnościach.

Aplikacje do testów stron i aplikacji internetowych posiadającej funkcje pozwalające na:

- przechwytywanie wszystkich zapytań i odpowiedzi pomiędzy przeglądarką a aplikacją docelową, nawet gdy używany jest HTTPS;
- przeglądanie, edytowanie oraz upuszczanie pojedynczych wiadomości, w celu manipulacji komponentami aplikacji po stronie serwera lub klienta;
- dodawanie adnotacji do poszczególnych elementów w celu ich oznaczenia do późniejszego sprawdzenia;
- wykonywanie różnych automatycznych modyfikacji odpowiedzi w calu ułatwienia testowania;
- tworzenie reguł dopasowywania i zastępowania do automatycznego stosowania własnych modyfikacji do żądań i odpowiedzi przechodzących przez serwer Proxy;
- precyzyjna konfiguracja reguł przechwytywania wiadomości;
- możliwość wyeliminowania ostrzeżeń bezpieczeństwa przeglądarki, mogących się pojawiać podczas przechwytywania połączeń HTTPS;
- pokazanie całej zawartości odkrytej podczas testowania umieszczana na mapie skanowanej witryny. Treść prezentowana w widoku drzewa, odpowiadającego strukturze stron URL;
- żądania i odpowiedzi dostępne w edytorze http;
- narzędzie do ręcznej edycji i ponownego wstawiania żądań;
- narzędzie do analizy statystycznej tokenów sesji;
- możliwość zapisu pracy na poszczególnych etapach w czasie rzeczywistym oraz powrót do zapisanego miejsca;
- biblioteka konfiguracji do szybkiego uruchomienia ukierunkowanego skanowania z różnymi ustawieniami;
- możliwość ręcznego umieszczania punktów wstawiania w dowolnych miejscach żądania, w celu poinformowania skanera o niestandardowych formatach danych i wejściach;

- skanowanie na żywo podczas przeglądania, zapewniające pełną kontrolę nad działaniami wykonywanymi dla żądań;
- możliwość analizy docelowej aplikacji internetowych.
- narzędzie do automatycznego przechwytywania szczegółowych wyników o niestandardowych atakach na aplikacje.

Potencjał osobowy przedstawia się poprzez posiadanie przez osoby testujące łącznie takich certyfikatów jak: OSCP (offensice security), CEH (EC-Council), Burp Suite Certified Practitioner (PortSwinger), eWPTX (eLearnSecurity), eCPPT (eLearnSecurity). Skanowania nie mogą być realizowane tylko z wykorzystaniem narzędzi automatycznych, konieczna jest manualna weryfikacja podatności znalezionych w testach automatycznych. Przeprowadzenie testów nie może wymagać od Zamawiającego zakupu żadnych dodatkowych licencji lub wyposażenia.

W ramach przeprowadzonych testów penetracyjnych infrastruktury, Wykonawca wykona:

1. Rekonesans.
    1. Zgromadzenie wszystkich dostępnych publicznie informacji nt. osób reprezentujących instytucję w celu stworzenia potencjalnej bazy loginów i haseł.
    2. Zgromadzenie informacji nt. zasobów instytucji dostępnych publicznie (strona internetowa, serwer www, serwer ftp, inne usługi).
    3. zgromadzenie informacji nt. potencjalnie niejawnych zasobów dostępnych dla wyszukiwarek internetowych.
    4. Sprawdzenie występowania w wyciekach znalezionych loginów.
2. Enumeracja zasobów.
    1. Analiza zasobów zidentyfikowanych w pkt. 1 w celu określenia precyzyjnej listy aplikacji (wraz z określeniem ich wersji) działających w ramach usług.
    2. Skanowanie publicznej infrastruktury.
    3. Skanowanie wewnętrznej infrastruktury z wykorzystaniem automatycznego skanera podatności.
    4. Sprawdzenie udostępnionych w sieci wewnętrznej plików i folderów w szczególności pod kątem występowania danych wrażliwych.
    5. Analiza dostępnych wewnątrz sieci, usług, protokołów i urządzeń.
3. Eksploatacja.
    1. Próba zalogowania do zidentyfikowanych zasobów, m.in. z użyciem list stworzonych w pkt. 1, także logowanie typu brute-force oraz domyślnych haseł.
    2. Wykorzystanie podatności ujawnionych na etapie enumeracji (cve dla znanych wersji aplikacji) - po uzgodnieniu z Zamawiającym.
    3. Analiza konfiguracji dostępnych środowisk w celu wykorzystania jej błędów (analiza hardeningu, architektury sieci, błędy w konfiguracji serwera www i architektury aplikacji internetowych oraz innych usług).
4. Eskalacja uprawnień.
    1. Wykorzystanie zasobów skompromitowanych w pkt. 3 w celu ewentualnego podniesienia uprawnień.
    2. Rozpoznanie zasobów wewnętrznych, przechodzenie na inne środowiska dostępne ze skompromitowanych w pkt.3 zasobów (lateral movement).

5. Raport z testu penetracyjnego.
   Wykonawca dostarczy raport zawierający:
   1. Podsumowanie dla kierownictwa.
   2. Opis zakresu wykonanych prac.
   3. Wyłączenia z testów, jeżeli były.
   4. Listę danych zebranych w trakcie rekonesansu (w tym listę zidentyfikowanych adresów IP w sieci wewnętrznej).
   5. Listę znalezionych podatności wraz z określoną dla niej wagą zgodnie z ze standardem Common Vulnerability Scoring System Version 4.0 oraz modelem STRIDE.
   6. Szczegółowy opis znalezionych podatności.
   7. Zalecenia naprawy nieprawidłowości bądź mitygacji zagrożeń z nich wynikających.