Opracowanie dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wraz z audytami(zerowym i końcowym) ramach projektu „Cyberbezpieczny samorząd”

OPIS PRZEDMIOTU ZAMÓWIENIA

Zakres rzeczowy:

Audyt zerowy zgodności z KRI, wdrożenie zaleceń po audycie, audyt końcowy zgodnie z KRI/ISO 27001 będzie obejmował realizację obowiązków, jakich od jednostki samorządu terytorialnego wymaga prawodawca. Usługa powinna obejmować:

Audyt zerowy zgodności z KRI

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / Krajowym Systemie Cyberbezpieczeństwa (KSC):
   - wyznaczenie osoby do kontaktu – Art. 21 KSC
   - przekazanie danych osoby wyznaczonej – Art. 22 pkt 5) KSC
   - zapewnienie zarządzania incydentem – Art. 22 pkt 1) KSC
   - zgłaszanie incydentu – Art. 22 pkt 2) Art. 23 KSC
   - zapewnienie obsługi incydentu – Art. 22 pkt 3) KSC
   - zapewnienie dostępu do wiedzy – Art. 22 pkt 4) KSC
   - opracowanie, ustanowienie i wdrożenie SZBI – Par. 20 KRI
   - monitorowanie i przegląd SZBI – Par. 20 KRI
   - doskonalenie SZBI – Par. 20 KRI
   - aktualizowanie regulacji wewnętrznych – Par. 20 pkt 1) KRI
   - inwentaryzacja sprzętu i oprogramowania – Par. 20 pkt 2) KRI
   - przeprowadzanie okresowych analiz ryzyka – Par. 20 pkt 3) KRI
   - postępowanie z ryzykiem – Par. 20 pkt 3) KRI
   - zarządzanie uprawnieniami – Par. 20 pkt 4), 5) KRI
   - szkolenia i uświadamianie – Par. 20 pkt 6) KRI
   - monitorowanie dostępu do informacji – Par. 20 pkt 7) a), b) KRI
   - monitorowanie nieautoryzowanych zmian – Par. 20 pkt 7) b) KRI
   - zabezpieczenie nieautoryzowanego dostępu – Par. 20 pkt 7) c) KRI
   - ustanowienie zasad bezpiecznej pracy mobilnej – Par. 20 pkt 8) KRI
   - zabezpieczenie informacji przed nieuprawnionym ujawnieniem – Par. 20 pkt 9) KRI
   - zabezpieczenie informacji przed nieuprawnioną modyfikacją – Par. 20 pkt 9) KRI
   - zabezpieczenie informacji przed nieuprawnionym usunięciem lub zniszczeniem – Par. 20 pkt 9) KRI
   - zawieranie w umowach serwisowych zapisów o bezpieczeństwie – Par. 20 pkt 10) KRI

- ustalenie zasad postępowania z informacjami w celu minimalizacji kradzieży informacji i środków przetwarzania – Par. 20 pkt 11) KRI
- aktualizowanie oprogramowania – Par. 20 pkt 12) a) KRI
- minimalizowanie ryzyka utraty informacji w wyniku awarii systemu – Par. 20 pkt 12) b) KRI
- ochrona systemu przed błędami – Par. 20 pkt 12) c) KRI
- stosowanie mechanizmów kryptograficznych w systemach – Par. 20 pkt 12) d) KRI
- zapewnienie bezpieczeństwa plików systemowych – Par. 20 pkt 12) e) KRI
- zarządzanie podatnościami systemów – Par. 20 pkt 12) f), g) KRI
- kontrola zgodności systemów z regulacjami – Par. 20 pkt 12) h) KRI
- zapewnienie audytu bezpieczeństwa informacji nie rzadziej niż raz na rok – Par. 20 pkt 14) KRI

2. Opracowanie raportu z audytu.

Wdrożenie SZBI

Wdrożenie warsztatowe Systemu Zarządzania Bezpieczeństwem Informacji, które będzie polegało na zapewnieniu zgodności z wymaganiami KRI zgodnie z powyższymi punktami oraz sposobem działania jednostki. Wdrożenie ma obejmować procesy, procedury, dokumenty. Powinno zostać przeprowadzane na podstawie wyników z audytu zerowego zgodności z KRI, który określi aktualny stan zgodności oraz wskaże punkty do doskonalenia.

Wdrożenie opiera się na: KRI, UoKSC, ISO27001, ISO22301.

Wynikiem wdrożenia jest wprowadzony System Zarządzania Bezpieczeństwem Informacji, który będzie wykorzystywany w jednostce oraz pozwoli zapewnić zgodność podczas audytu końcowego.

Audyt końcowy zgodności z KRI/ISO 27001 + uzupełnienie załącznika nr 6

1. Ocena zgodności z Krajowymi Ramami Interoperacyjności (KRI) / normy ISO 27001
2. Opracowanie raportu z audytu
3. Uzupełnienie załącznika nr 6 – ankieta dojrzałości cyberbezpieczeństwa w jednostkach samorządu terytorialnego (Urząd Gminy Człuchów, Zakład Gospodarki Komunalnej przy UG Człuchów, Gminny Ośrodek Pomocy Społecznej).

Testy penetracyjne, socjotechniczne + security awareness

W ramach działań związanych z zarządzaniem podatnościami oraz podnoszeniem wiedzy pracowników w zakresie cyberbezpieczeństwa usługa testów penetracyjnych infrastruktury sieciowej wraz z testami socjotechnicznymi według poniższego planu.

Testy muszą być wykonane manualnie i automatycznie, wyklucza się wykonanie tylko skanów podatności oraz same działania automatyczne.

1. Testy penetracyjne infrastruktury sieciowej:
    a. weryfikacja podatności i luk bezpieczeństwa
    b. poszukiwanie zero day'ów
    c. próba przełamania haseł
    d. próba podniesienia uprawnień
    e. weryfikacja potencjalnych wektorów ataku
    f. skanowanie infrastruktury

g. próba wylistowania użytkowników
h. poszukiwanie otwartych portów

2. Kampania phishingowa, według ustalonego scenariusza
3. Przygotowanie raportu zawierającego:
   a. listę podatności,
   b. poziom zagrożenia
   c. opis podatności
   d. szczegóły występowania + szczegóły techniczne
   e. rekomendacje
   f. referencje
4. Wsparcie po audytowe – polegające na pomocy zrozumienia podatności oraz stopnia jego wpływu na organizację. Dodatkowe wsparcie przy określaniu rekomendacji.

Wymagania dla Wykonawcy:

1. Certyfikaty (co najmniej 2 audytorów posiadających, każdy z nich co najmniej jeden z certyfikatów):

- Certified Internal Auditor (CIA);
- Certified Information System Auditor (CISA);
- 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;
- 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;
- Certified Information Security Manager (CISM);
- Certified in Risk and Information Systems Control (CRISC);
- Certified in the Governance of Enterprise IT (CGEIT);
- Certified Information Systems Security Professional (CISSP);
- Systems Security Certified Practitioner (SSCP);
- Certified Reliability Professional;
- Certyfikaty uprawniające do posiadania tytułu ISA/IEC 62443 Cybersecurity Expert.

2. Wykonane audyty : w ciągu ostatnich dwóch lat wykonał co najmniej 3 audyty bezpieczeństwa informacji oraz co najmniej 3 usługi testów penetracyjnych.
3. Posiadane certyfikaty dla organizacji: Wykonawca ma wdrożone i może to potwierdzić posiadanym certyfikatem:

- ISO 27001
- ISO 22301
- ISO 9001
- WSK (Wewnętrzny System Kontroli)
- Koncesja MSWiA