Załącznik 1 do Zapytania Ofertowego

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest usługa przeprowadzenia audytu Systemu Zarządzania Bezpieczeństwem Informacji wdrożonego w Urzędzie Miejskim w Łowiczu na zgodność z wymaganiami:

1. Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077).
2. Normy PN-EN ISO/IEC 27001:2023-08
3. 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. poz. 773).

Miejsce audytu: Urząd Miejski w Łowiczu
Przeprowadzenie audytów w ramach niniejszego zamówienia musi odbyć się na miejscu, po przeprowadzeniu szczegółowej wizji lokalnej oraz po szczegółowym zapoznaniu się z posiadanymi dokumentami/warunkami/systemami, które zostaną udostępnione tylko w siedzibie Zamawiającego.

Zakres audyt
Wykonawca jest zobowiązany do przeprowadzenia audytu wdrożonego u Zamawiającego systemu zarządzania bezpieczeństwem informacji, w związku z obowiązkiem ciążącym na kierownictwie podmiotu publicznego zgodnie z zapisami w § 19 ust. 2 pkt 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 (Dz. U. poz. 773)., zwanego dalej „rozporządzeniem KRI", w zakresie obejmującym zgodność z kryteriami zawartymi w § 20 ust. 2 rozporządzenia KRI oraz zgodność z wymaganiami normy PN-ISO/IEC 27001:2023-08
W zakresie przedmiotu zamówienia jest także obowiązek świadczenia przez Wykonawcę wsparcia poaudytowego przez okres 12 miesięcy, które polegać będzie m.in. na: udzielanie informacji na temat zaleceń audytowanych oraz rekomendowanych sposobów podejścia do rozwiazywania zagadnień w obszarze cyberbezpieczeństwa, które pojawią się w związku z działalnością urzędu.

Audyt zgodności musi obejmować w szczególności:

1. weryfikację bezpieczeństwa fizycznego (sprawdzenie ochrony pomieszczeń, sprzętów, infrastruktury oraz personelu przed bezpośrednim działaniem czynników fizycznych i zdarzeń takich jak kradzież, nieuprawniony dostęp),
2. weryfikację bezpieczeństwa informatycznego (analiza bezpieczeństwa systemu teleinformatycznego)
3. weryfikację bezpieczeństwa organizacyjnego (stosowane procedury bezpieczeństwa), w tym przegląd dokumentacji dotyczącej systemu zarządzania bezpieczeństwem informacji.
4. analizę stanu bezpieczeństwa informacji
5. ocenę wdrożonych systemów zabezpieczeń i procedur
6. zebranie dowodów audytowych
7. wskazanie wykrytych podatności, uchybień oraz błędów
8. zdefiniowanie rekomendowanych działań korygujących w zakresie objętym audytem,
9. zdefiniowanie rekomendacji dotyczących działań naprawczych i usprawnień

Po wykonaniu prac audytowych, Wykonawca zobowiązany jest do dostarczenia Zamawiającemu Raportu z audytu bezpieczeństwa systemu informacyjnego, zgodne z ustawą o krajowym systemie cyberbezpieczeństwa wraz z wytycznymi i rekomendacjami rozwiązań, które należy wdrożyć, aby dostosować Zamawiającego do wymagań kryteriów audytu.
Szczegółowe wymagania co do zakresu Raportu, zostały opisane w Załączniku 1 do niniejszego OPZ

Wymagania co do audytorów
Zamawiający wymaga aby audyt przeprowadziły osoby dysponujące stosowną wiedzą i kwalifikacjami, za które Zamawiający uznaje osoby posiadające 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 (t.j. Dz. U. z 2022 r. poz. 1854 z późn. zm.), w zakresie certyfikacji osób, o którym mowa w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu wydanym na podstawie art. 15. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077). osób przeprowadzających audyt.
Zamawiający wymaga by do przedłożonego Zamawiającemu Raportu z audytu były dołączone kopie w.w. certyfikatów.

Zamówienia jest realizowane w ramach projektu „Podniesienie poziomu cyberbezpieczeństwa w Urzędzie Miejskim w Łowiczu" współfinansowanego na podstawie umowy o powierzenie grantu o numerze FERC.02.02-CS.01-001/23/0333/FERC.02.02-CS.01-001/23/2024.

Załącznik 1 do Zapytania Ofertowego

Zakres Raportu z audytu

Raportu z audytu powinien zawierać w szczególności opis:

1. zidentyfikowanych systemów informacyjnych służących do świadczenia usług przez Zamawiającego
2. zidentyfikowanych systemów oraz narzędzi wspierających system informacyjny do świadczenia usług
3. stosowanej procedury administrowania świadczonymi usługami oraz systemem informacyjnym
4. organizacji wewnętrznej struktury cyberbezpieczeństwa
5. wykazu osób odpowiedzialnych za utrzymanie kontaktów z podmiotami KSC
6. sposobu szacowania ryzyka dla systemu informacyjnego
7. sposobu szacowania ryzyka dla obiektu, w którym zlokalizowane są systemy informacyjne
8. organizacji systemu zarządzania bezpieczeństwem informacji (ISO 27001)
9. stosowanych zabezpieczeń systemu zarządzania bezpieczeństwem informacji (ISO 27001) (Załącznik A)
10. organizacji zarządzania ciągłością działania (ISO 22301):
11. sposobu zbierania informacji o zagrożeniach dla systemów informacyjnych i ich podatnościach
12. monitorowania systemu informacyjnego
13. sposobu zabezpieczenia dokumentacji dotyczącej cyberbezpieczeństwa
14. sposobu zarządzania incydentami
15. stosowanych sposobów:
    15.1. analizy kodu złośliwego
    15.2. badania odporności systemu informacyjnego
    15.3. zabezpieczenia śladów kryminalistycznych
16. stosowanych modeli oraz środków łączności wewnętrznej i zewnętrznej,
17. stosowanych zabezpieczeń przed utratą i kradzieżą danych
18. stosowanych sposobów kontroli dostępu do systemów informatycznych, w tym dostępu przez usługi i narzędzia zdalne
19. procedur i środków technicznych stosowanych dla zabezpieczeń przy pracy zdalnej
20. technicznej infrastruktury w systemach ICT, schematu sieci, a także zabezpieczeń sieci.
21. procedur i środków technicznych stosowanych dla zabezpieczeń dostępu do sieci publicznej
22. procedur i środków technicznych stosowanych dla zabezpieczeń wewnętrznej sieci ICT
23. systemu identyfikowania i uwierzytelniania użytkowników i administratorów
24. procedur i środków technicznych stosowanych dla backupów i archiwizacji danych, w tym testów odtworzeniowych,
25. zidentyfikowanych pojedynczych punktów awarii
26. procedur i środków technicznych stosowanych dla zapewnienia ciągłości pracy systemów i sieci
27. stosowanych systemów zabezpieczeń kryptograficznych
28. sposobu szyfrowania danych przechowywanych poza siedzibami Zamawiającego, w tym m.in. serwisy pocztowe email, serwisy WEB itp.
29. zabezpieczeń komputerów przed atakami phishingowymi
30. systemów ochrony poczty email i usług WEB pod kątem ataków phishingowych
31. procedur i środków technicznych stosowanych dla ochrony ICT przed oprogramowaniem szkodliwym, w tym weryfikacji zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania
32. procedur i środków technicznych stosowanych dla zapisów historii zmian w dokumentach, systemach informatycznych itp.
33. procedur i środków technicznych stosowanych dla zarządzania i zabezpieczania nośników przechowujących dane
34. zasad odpowiedzialności użytkowników
35. zasad zarządzania hasłami
36. procedur i środków technicznych stosowanych przy niszczeniu niepotrzebnych nośników i danych
37. wyników weryfikacji stron webowych pod kątem zgodności ze standardem WCAG 2.1
38. sposobu zbierania logów, zakresu i retencji logów
39. zaangażowania kierownictwa w proces ciągłego doskonalenia systemu bezpieczeństwa informacji.
40. wyników przeprowadzonego przez Wykonawcę badania podatności usług sieciowych i całej infrastruktury ICT, wykonanego z użyciem testów penetracyjnych, zgodnie z wymaganiami określonymi w Załączniku TP;

Załącznik 1 do Zapytania Ofertowego

Wymagania w zakresie przeprowadzenia i udokumentowania testów penetracyjnych

I. Wykonawca w ramach testów penetracyjnych wykona:

1. Zewnętrzne testy bezpieczeństwa urządzeń sieciowych obejmujące:
   - 1.1. Zbadanie odporności urządzeń na ataki z poziomu Internetu;
   - 1.2. Wskazanie potencjalnych skutków ataku dla znalezionych luk i określenie ich krytyczności;
   - 1.3. Analizę podatności na ataki;
   - 1.4. Skanowanie portów TCP / UDP;
   - 1.5. Skanowanie hostów aktywnych w danej podsieci;
   - 1.6. Określenie ścieżki sieciowej do urządzenia;
   - 1.7. Próbę detekcji typu oraz wersji usług sieciowych działających w systemie;
   - 1.8. Próbę detekcji wersji oraz typu oprogramowania systemowego zainstalowanego na urządzeniu
   - 1.9. Po udanej detekcji wersji oprogramowania systemowego / usług – próbę lokalizacji znanych podatności w danych wersjach oprogramowania;
   - 1.10. Próbę komunikacji w obrębie protokołu ICMP;
2. Wewnętrzne testy penetracyjne obejmujące:
   - 2.1. Bezpieczeństwo urządzeń sieciowych;
   - 2.2. Bezpieczeństwo protokołów trasowania;
   - 2.3. Analiza topologii sieci i logiki jej segmentacji;
   - 2.4. Bezpieczeństwo maszyn zlokalizowanych w obrębie sieci (serwery, stacje robocze);
   - 2.5. Bezpieczeństwo usług zlokalizowanych na każdym z dostępnych w sieci urządzeniu oraz maszynie, istnienie nieautoryzowanych urządzeń (np. nieautoryzowanego urządzenia bezprzewodowego wpiętego do sieci);
   - 2.6. Filtrowanie komunikacji wewnętrznej (np. konfiguracja firewall, IDS/IPS, WAF, separacja kluczowych podsieci);
   - 2.7. Konfiguracja komunikacji z zasobami (np. konfiguracja SSL/TLS dla kluczowych aplikacji);
   - 2.8. Możliwość uzyskania nieautoryzowanego dostępu do danych (np. danych wrażliwych);
   - 2.9. Przegląd danych dostępnych na udziałach sieciowych –możliwość uzyskania nieautoryzowanego dostępu do danych na udziałach sieciowych, hasła do systemów, czy kluczowych dla działania organizacji danych.

II. Testy penetracyjne muszą zweryfikować istnienie minimum następujących rodzin podatności:

lp.	podatność	lp.	podatność
1.	AIX Local Security Checks	28.	Mobile Devices
2.	Amazon Linux Local Security Checks	29.	Netware
3.	Backdoors	30.	NewStart CGSL Local Security Checks
4.	Brute force attacks	31.	Oracle Linux Local Security Checks
5.	CGI abuses	32.	OracleVM Local Security Checks
6.	CGI abuses : XSS	33.	Palo Alto Local Security Checks
7.	CISCO	34.	Peer-To-Peer File Sharing
8.	CentOS Local Security Checks	35.	PhotonOS Local Security Checks
9.	DNS	36.	Policy Compliance
10.	Databases	37.	Port scanners
11.	Debian Local Security Checks	38.	RPC
12.	Default Unix Accounts	39.	Red Hat Local Security Checks
13.	Denial of Service	40.	SMTP problems
14.	F5 Networks Local Security Checks	41.	SNMP
15.	FTP	42.	Scientific Linux Local Security Checks
16.	Fedora Local Security Checks	43.	Service detection
17.	Firewalls	44.	Settings
18.	FreeBSD Local Security Checks	45.	Slackware Local Security Checks
19.	Gain a shell remotely	46.	Solaris Local Security Checks
20.	General	47.	SuSE Local Security Checks
21.	Gentoo Local Security Checks	48.	Ubuntu Local Security Checks
22.	HP-UX Local Security Checks	49.	VMware ESX Local Security Checks
23.	Huawei Local Security Checks	50.	Virtuozzo Local Security Checks
24.	Junos Local Security Checks	51.	Web Servers
25.	MacOS X Local Security Checks	52.	Windows
26.	Mandriva Local Security Checks	53.	Windows : Microsoft Bulletins
27.	Misc.	54.	Windows : User management