URZĄD MIASTA TORUNIA
Biuro Projektów Informatycznych
ul. Wały gen. Sikorskiego 10
87-100 Toruń

Pytanie 1:
Czy posiadacie Państwo wdrożone elementy systemu ISO 27001? jak tak, to jakie?

Odpowiedź 1:
Weryfikacja posiadanych przez UMT procedur i instrukcji oraz ich zgodności z ISO jest elementem zapytania. Celem jest zbudowanie całościowego systemu zarządzania bezpieczeństwem informacji.

Pytanie 2:
Czy możecie Państwo przedstawić spis posiadanych zasobów i przypisanych właścicieli?

Odpowiedź 2:
Zamawiający nie posiada takiego zestawienia

Pytanie 3:
Ile osób ma obejmować szkolenie, w jakiej formie ma być przeprowadzone. Co w chwili obecnej składa się na dokumentację Państwa?

Odpowiedź 3:
Szkolenie ma obejmować wszystkich pracowników UMT (obecnie 450 osób)
Weryfikacja posiadanej dokumentacji jest elementem zapytania.

Pytanie:
Czy posiadacie Państwo system nadzoru zainstalowanego oprogramowania na komputerach służbowych?

Odpowiedź 4:
Na komputerach służbowych obecnie używane jest oprogramownaie LogPlus

Pytanie 5:
W nawiązaniu do pkt.: 3.a.xii - czy rozumie się przez to działania red teamowe?

Odpowiedź 5:
Zamawiający oczekuje propozycji metod prowadzenia testów, nie wyklucza również metod opartych o prowokacje.

Pytanie 6:
W nawiązaniu do pkt.: 3.b.xiv - czy wykorzystywana kryptografia opiera się o rozwiązania dostępne na rynku, czy jest to Państwa autorskie rozwiązanie?

Odpowiedź 6:
O rozwiązania dostępne na rynku.

Pytanie 7:
Ile urządzeń jest w domenie?

Odpowiedź 7:
W domenie są 3 kontrolery domeny, 800 wpisów stacji roboczych, 600 kont.

Pytanie 8:
Czy posiadacie Państwo rejestr incydentów (bezpieczeństwa fizycznego, IT, RODO)

Odpowiedź 8:
Tak. Rejestr naruszeń ochrony danych osobowych

Pytanie 9:
pkt C)I. - Prosimy o wytłumaczenie co jest rozumiane jako system informatyczny oraz co rozumiemy jako podłączenie się ze stacji roboczej z zewnątrz. Czy mowa tutaj o testach penetracyjnych usług wystawionych zewnętrznie?

Odpowiedź 9:
Przez system informatyczny Zamawiający rozumie urządzenie (lub grupa urządzeń np. klaster z macierzą) wraz z oprogramowaniem np. końcowa stacja robocza UMT.
Stacja robocza z zewnątrz – urządzenie nie wpięte do sieci UMT. Mowa jest o testach penetracyjnych.

Pytanie 10:
C) III - Prosimy o wskazanie szacunkowej liczby urządzeń oraz usług udostępnianych do sieci zewnętrznej. Jaka będzie ilość usług/urządzeń podlegająca testom.

Odpowiedź 10:
30 usług, 10 urządzeń

Pytanie 11:
C) IV - Prosimy o wskazanie szacunkowej liczby urządzeń w sieci wewnętrznych. Jaka będzie ilość usług/urządzeń podlegająca testom.

Odpowiedź 11:
700 stacji roboczych, 230 maszyn wirtualnych

Pytanie 12:
C) VIII - Dla ilu serwerów/stacji powinno zostać przeprowadzone badanie ochrony przed szkodliwym oprogramowania

Odpowiedź 12:
700 stacji roboczych, 230 maszyn wirtualnych

13. Dodatkowo:
Pytanie: Ilość podsieci w organizacji

Odpowiedź: 30

Pytanie: Ilość stacji roboczych, użytkowników, serwerów, drukarek, routerów, switchy, dodatkowych urządzeń itp.

Odpowiedź: 700 stacji roboczych, 230 maszyn wirtualnych, 500 użytkowników

Pytanie: Czy organizacja korzysta z rozwiązań pozwalających na pracę zdalną (VPN)?

Odpowiedź: Tak

Pytanie: Czy organizacja korzysta z rozwiązań chmurowych, jeżeli tak to jakich?

Odpowiedź: Nie

Pytanie: Ilość sieci WiFi oraz to czy mają one podlegać testom?

Odpowiedź: 2 sieci - Tak

Pytanie: Czy w organizacji używane jest Active Directory?

Odpowiedź: Tak

Pytanie: Ilość fizycznych lokalizacji - czy wszystkie lokalizacje są wpięte do jednej sieci wewnętrznej? np. w ramach Active Directory (forest, tree)?

Odpowiedź: 15 lokalizacji wpiętych do 1 sieci

Pytanie: Czy organizacja posiada serwery, komputery zlokalizowane w infrastrukturze dostawcy zewnętrznego?

Odpowiedź: Nie

Pytanie: W pkt 8.D o szkoleniu personelu – Prośba o doprecyzowanie - co jest rozumiane w tym pkt i jaki jest tego zakres?

Odpowiedź : Przeprowadzenie szkolenia stacjonarnego (w pomieszczeniach UMT) dla wszystkich pracowników i kadry zarządzającej z Dokumentacji SZBI przygotowanej przez oferenta oraz z podstawowych wymagań normy ISO/IEC 27001, Krajowych Ramy Interoperacyjności, Ogólnego rozporządzenia o ochronie danych oraz Dyrektywy NIS2.

Zamawiający przesuwa termin składania ofert do dnia 29.08.2024 r. do godz. 14:00

Główny Specjalista

Grzegorz Hrynek