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

Pytanie 14:
Ilość lokalizacji Urzędu (adresy, info. co znajduje się pod danym adresem – jakie Wydziały, Referaty, Filie itp.)

Odpowiedź 14:
15okalizacji – szczegółowe informacje znajdują się na bip.um.torun.pl

Pytanie 15:
Ilość pracowników/użytkowników

Odpowiedź 15:
Zatrudnionych jest ok. 500 osób

Pytanie 16:
Ilość wszystkich hostów podłączonych do sieci (komputery, urządzenia serwerowe, urządzenia sieciowe jak np. drukarki, routery, przełączniki, Access Pointy, urządzenia VoIP etc.). W tym rozgraniczyć:

a. Ilość komputerów (również przenośnych)
b. Ilość serwerów (fizycznych, wirtualnych)
c. Ilość pozostałych urządzeń podłączonych do sieci

Odpowiedź 16:
800 stacji roboczych. 230 maszyn wirtualnych, 15 fizycznych do weryfikacji w ramach audytu

Pytanie 17:
Ilość adresów zewnętrznych/publicznych

Odpowiedź 17:
68 adresów

Pytanie 18:
Ilość podsieci (jaki zakres maski każdej podsieci?)

Odpowiedź 18:
30 podsieci

Pytanie 19:
Ilość serwerowni i ich lokalizacja?

Odpowiedź 19:
10 serwerowni (w tym 4 kluczowe)

Pytanie 20:
Czy mają Państwo wdrożoną Active Directory?

Odpowiedź 20:
Tak

Pytanie 21:
Czy testy penetracyjne da się zrobić z budynku Urzędu, czy trzeba fizycznie odwiedzić każdą lokalizację w mieście? (Jeśli testy trzeba wykonać na wszystkich hostach)

Odpowiedź 21:
Fizycznie trzeba odwiedzić każdą lokalizację, testy penetracyjne można zrobić z 1 lokalizacji.

Pytanie 22:
Czy testom penetracyjnym mają być poddane wszystkie wymienione w pyt. 3-6 hosty, adresy zewnętrzne, podsieci, czy przewidują Państwo jakąś konkretną próbę – jeśli próba, to proszę o konkretne wskazanie powyższych ilości do próby oraz lokalizacji gdzie testy mają się fizycznie odbyć.

Odpowiedź 22:
Wszystkie. Testy będą przeprowadzane z siedziby Biura Projektów Informatycznych

Pytanie 23:
Jakie adresy www/serwisy internetowe mają być poddane badaniu podatności?

Odpowiedź 23:
Wszystkie serwisy UMT

Pytanie 24:
Czy licencje są gromadzone w jednym miejscu i mają Państwo wspólny udział sieciowy, do którego można podłączyć skaner, czy trzeba skanować każdą stację roboczą osobno?

Odpowiedź 24:
Zamawiający posiada oprogramowanie do nadzoru zainstalowanego oprogramowania na komputerach służbowych

Pytanie 25:
Czy są w użytku licencje pudełkowe, czy tylko elektroniczne?

Odpowiedź 25:
Zamawiający używa zarówno jednych jak i drugich

Pytanie 26:
Jakie systemy operacyjne są na stacjach roboczych i serwerach?

Odpowiedź 26:
Systemy rodziny Windows oraz Linux – do weryfikacji w ramach audytu

Pytanie 27:
Jeżeli chodzi o aktualizację/opracowanie dokumentacji SZBI KRI/KSC/ISO27001/NIS2 - czy przygotowanie dokumentacji ma być NA ZGODNOŚĆ z normą ISO27001 literalnie punkt po punkcie, celem późniejszej CERTFIKACJI Urzędu, czy ma to być W OPARCIU o dobre praktyki zaczerpnięte z normy i pozostałych wymienionych aktów prawnych w takim zakresie aby spełniać ich wymogi?

Odpowiedź 27:
Przygotowana dokumentacja ma spełniać wszystkie wymagania wymienionych przepisów, norm i regulacji być oparta o dobre praktyki (również ITIL) oraz umożliwiać certyfikację.

Pytanie 28:
Jaką dokumentację bezpieczeństwa aktualnie Państwo posiadają (np. polityka bezpieczeństwa informacji, polityka zarządzania incydentami, polityka szacowania ryzyka, instrukcja zarządzania incydentami itp. dokumenty, czy dokumenty opisane w samym zapytaniu, proszę wymienić). Kiedy była ostatni raz aktualizowana?

Odpowiedź 28:
Weryfikacja posiadanych przez UMT procedur i instrukcji oraz ich zgodności z ISO jest elementem zapytania. Celem jest zbudowanie całościowego systemu zarządzania bezpieczeństwem informacji.

Pytanie 29:
W zakresie audytu pojawia się Audyt RODO ale nie widać aby była do zrobienia przez Wykonawcę dokumentacji związana z RODO - czy tym obszarem zajmuje się Państwa IOD i nie potrzeba wchodzić w Jego kompetencje, jeśli chodzi o aktualizacją polityki RODO, rejestru czynności przetwarzania itd.? (czy taka dokumentacja może mieści się w punkcie IX. niniejszego szacowania?

Odpowiedź 29:
Weryfikacja posiadanych przez UMT procedur i instrukcji oraz ich zgodności z RODO jest elementem zapytania. Celem jest zbudowanie całościowego systemu zarządzania bezpieczeństwem informacji.

Główny Specjalista
Grzegorz Hrynek