

OPIS PRZEDMIOTU ZAMÓWIENIA

na usługę audytu informatycznego systemu sprzedaży operatora, sprzedającego w imieniu ZTM bilety uprawniające do korzystania z usług lokalnego transportu zbiorowego w Warszawie.

Przedmiot zamówienia obejmuje zbadanie obszarów bezpieczeństwa, będących przedmiotem usługi sprzedaży biletów, zgodnie z następującym zakresem prac:

1. Audyt systemu sprzedażowego
 - a. ocena procedur przygotowujących proces sprzedaży (konfiguracja, parametryzacja),
 - b. ocena procedur opisujących i regulujących procesy sprzedażowe,
 - c. ocena sprawności procesu sprzedaży biletu na wskazanych przez Zamawiającego urządzeniach,
 - d. procedura kontrolna polegająca analizie procesu sprzedaży na wskazanych przez Zamawiającego urządzeniach,
2. Audyt mechanizmów uwierzytelniania
 - a. ocena kontroli dostępu do systemu sprzedażowego oraz do urządzeń sprzedażowych, systemu plików baz danych, aktualizacja uprawnień, poziomy uprawnień, weryfikacja przypisanych uprawnień,
 - b. ocena mechanizmów rejestracji wejść,
3. Audyt ochrony integralności danych
 - a. jak jest weryfikowana kompletność przesyłanych danych,
 - b. czy urządzenia mają możliwość przechowywania większej ilości danych w przypadku braku łączności i ewentualnie w jakim okresie mogą one być przechowywane w sposób bezpieczny,
 - c. tryb pracy urządzenia w przypadku braku łączności,
4. Audyt, weryfikacja i ocena zaimplementowanych systemów logowania zdarzeń,
5. Audyt obsługi błędów
 - a. jak są raportowane błędy w działaniu urządzeń,
 - b. czy raporty o usterkach obejmują wszystkie problemów jakie pojawiają się w urządzeniach (np. wyczerpanie się dostępnej puli numerów biletów),
 - c. czy raportowane są informacje na temat aktualnej taryfy w automacie oraz zakresu dostępnej wykorzystanej i niewykorzystanej numeracji ,
 - d. czy istnieje możliwość zweryfikowania czy w urządzeniu jest prawidłowa wersja oprogramowania,
6. Audyt raportowania
 - a. jak jest monitorowana praca urządzenia,
 - b. jak są tworzone raporty (automatycznie, ręcznie),
 - c. czy raporty generowane są zgodnie z umową, czy jest rejestrowane generowanie raportu i jego wysyłka,
 - d. czy pliki tekstowe (techniczne) ze szczegółowymi informacjami o zrealizowanej sprzedaży generowane automatycznie czy ręcznie,
 - e. czy jest rejestrowane generowanie plików tekstowych (technicznych) i ich wysyłka,
 - f. czy kontrolowana jest integralność danych zawartych w plikach tekstowych (technicznych),

- g. czy aplikacja zarządzająca obejmuje wszystkie urządzenia i jest wystarczająca dla racjonalnego monitorowania ciągłości sprzedaży, przydziału pul nr biletów, udzielania informacji o awariach i usterkach, raportowania danych o sprzedaży.
7. Audyt gospodarki kartami SAM
 - a. czy jest prowadzony rejestr kart SAM z przypisaniem do danego urządzenia, z uwzględnieniem migracji kart
 - b. czy jest dostępny archiwalny wykaz kart SAM przypisanych do urządzeń,
 - c. czy dane o przypisaniu karty SAM do urządzenia są generowane automatycznie,
 - d. ocena procedur zabezpieczeń w zakresie nieużywanych kart SAM,
 8. Audyt serwisu urządzeń
 - a. Czy są stosowane procedury serwisowe. Ocena zakresu oraz stosowania procedur obsługi serwisowej,
 - b. czy jest prowadzony rejestr czynności serwisowych, oraz czy jest weryfikowany sposób zrealizowania zadania serwisowego,
 - c. ocena wpływu czynności serwisowych na integralność danych,
 - d. czy czynności serwisowe są podejmowane zgodnie z umową,
 - e. czy dane logowania serwisanta są rejestrowane w pamięci urządzenia lub w formie innego dedykowanego rejestru.
 9. Zbadanie na podstawie rzeczywistych danych dostarczonych do audytu przez Zamawiającego za okres 3 ostatnich lat całego procesu sprzedaży oraz raportowania.
 - a. Sprawdzenie czy wszystkie dane rzeczywiste dostarczone do audytu przez Zamawiającego znajdują odzwierciedlenie w audytowanych systemach,
 - b. Sprawdzenie czy wszystkie dane znajdujące się w audytowanych systemach są właściwie raportowane,
 - c. Sprawdzenie czy raporty sprzedażowe zarówno finansowe jak i techniczne dostarczane do Zamawiającego z audytowanych systemów zawierają powyższe dane,
 - d. Sprawdzenie procesu tworzenia danych wynikowych do Zamawiającego (plików technicznych, raportów finansowych i sprzedażowych), jego kompletności, integralności, możliwości ręcznej ingerencji,
 - e. Sprawdzenie kompletności danych sprzedażowych w online-owym systemie dostarczonym do ZTM, potwierdzenie zgodności zawartych w nim danych z audytowanymi systemami.
 10. Występowanie nieprawidłowości spowodowanych błędem lub celowym działaniem człowieka we wszystkich powyższych obszarach.
 11. Do oferty Wykonawca musi załączyć:
 - a. certyfikat audytora wiodącego w zakresie stosowania wytycznych normy PN-EN ISO/IEC 27001:2017-06,
 - b. udokumentowanie minimum 5-letniego doświadczenia w prowadzeniu działań audytowych,
 - c. udokumentowanie znajomości podstawowych technik programowania aplikacji internetowych oraz bazodanowych.