Dobre praktyki bezpieczeństwa w obszarze transakcji kartowych

Niniejsze „Dobre praktyki” powinny być stosowane w ramach bieżącej działalności Firmy, a szczególnie płatności kartowych, ich monitoringu oraz rekoncyliacji transakcji.

W obszarze płatności kartowych:

1. Procesy każdego programu kartowego powinny działać w oparciu o właściwą umowę i regulamin, a także zasady takie jak:
    a. transakcja, w ramach której dane karty są użyte do bezpośredniego zainicjowania płatności, powinna być zlecana tylko przez Posiadacza tej karty,
    b. jeśli standard transakcji wymaga przekazania danych karty w ramach otwartych kanałów takich jak e-mail lub telefon (tj. transakcja typu MOTO), dane powinny być przekazane bezpośrednio do Akceptanta, bez dostępu do nich przez osoby trzecie.
2. Zwroty powinny być dokonywane w taki sposób, w jaki nastąpiła płatność (tj. na dany instrument, który został użyty do dokonania płatności).
3. W przypadku dużej transakcyjności na pojedynczych kartach, sugerujemy rozważenie wydania co najmniej 1 dodatkowej karty dla każdego z Posiadaczy Kart i ich wymiana naprzemiennie w krótkich terminach, np. co 6 miesięcy.
4. Dodatkowe zawężenie miejsc, w których można dokonać płatności kartą (za pomocą określenia dozwolonych lub wykluczonych kodów MCC (merchant category code) czyli czterocyfrowych oznaczeń nadawanych podmiotom przyjmującym płatności określających typ biznesu prowadzonego przez podmiot – odbiorcę płatności) do typowych lub spodziewanych wydatków, jeśli wykorzystywane są karty z wysokimi limitami lub dedykowane dla specyficznych płatności/odbiorców.

   Przykład: W przypadku firm z branży turystycznej karty powinny działać tylko u sprzedawców z danej branży, a nawet zgodnie ze specyfiką działań poszczególnych zespołów, np. karty działu lotniczego powinny mieć możliwość płacenia tylko za bilety lub usługi lotnicze.
5. Systemy/serwisy/internetowe strony transakcyjne używane przez Firmę – używanie karty z zamaskowanymi danymi lub z niskim limitem, jeśli dane karty mogą być widoczne przez osoby trzecie.
6. Limity kart powinny odpowiadać najczęstszej wartości transakcji. Dla wyższych i rzadszych kwot, zmiana limitu może odbywać się w trybie on-line poprzez moduł OLM w systemie CitiManager. Zmiana taka powinna być czasowa, a limit karty/transakcji przywrócony do pierwotnego poziomu po dokonaniu płatności.
7. Uwzględnienie w limitach kart i transakcji możliwości złożenia chargeback’ów, których ilość może być limitowana (zasady i limity dotyczące chargeback określa organizacja kartowa np. Visa, przy czym Bank nie ma wpływu na ustalanie tych zasad i limitów przez organizacje kartowe).
8. Dokonywanie transakcji typu MOTO (mail order, telephone order) tylko tam, gdzie nie ma innej możliwości dokonania płatności.
9. Limity dopasowane do różnych działów w Firmie i typów płatności - dla przykładu w przypadku firmy z branży turystycznej karty działu np. rezerwacji hotelowych powinny mieć inne wartości limitów całkowitych i limitów pojedynczych transakcji, niż karty działu zakupu biletów lotniczych.

W zakresie monitoringu transakcji kartowych:

1. Bieżąca analiza transakcji w autoryzacji widocznych w CitiManager (status widoczny przed obciążeniem karty w trybie on-line). Analiza transakcji w autoryzacji pozwala na wychwycenie transakcji oszukańczej przed zaksięgowaniem jej w ciężar karty.
2. Bieżąca analiza transakcji zaksięgowanych na karcie widocznych w CitiManager.
3. Bieżąca analiza powiadomień o każdej wysokokwotowej transakcji oraz osiągnięciu wysokiego wykorzystania limitu karty. CitiManager pozwala na wysyłanie powiadomień w trybie on-line do 5 różnych odbiorców, w wielu wariantach, jak np. powiadomienie o każdej transakcji, o transakcji powyżej kwoty X, czy wykorzystaniu limitu do X%.
4. Monitorowanie, czy dany sprzedawca (merchant) jest na liście sprzedawców, z którymi Firma przeprowadza transakcje. Kontrola nie powinna ograniczać się tylko do weryfikowania, czy typ sprzedawcy jest charakterystyczny dla danego działu.
5. Każdorazowa blokada karty w przypadku próby albo obciążenia transakcją, która nie jest znana.
6. W chwili zidentyfikowania transakcji oszukańczej, bezzwłoczny kontakt ze sprzedawcą w celu anulowania lub zablokowania usługi i zwrotu płatności.

Dotyczące procesu rekoncyliacji:

1. Rekoncyliacja danych z zaksięgowanych transakcji w systemie CitiManager lub CitiManager Reporting z dokonanymi rezerwacjami/zleceniami w trybie dziennym, niezwłocznie po ich udostępnieniu w systemie Banku.
2. Automatyzacja procesów w oparciu o integracje systemowe pomiędzy Bankiem a Firmą.

Bank zastrzega sobie prawo do wycofania, ograniczenia lub zmiany warunków obecnej współpracy w dowolnym momencie na podstawie dalszych procesów transakcyjnych. Materiał ten nie jest przeznaczony do poufnego użytku i zawarte w nim wskazówki mogą zostać przekazane innym odbiorcom w celu zwiększenia bezpieczeństwa transakcji dokonywanych instrumentami płatniczymi oferowanymi przez bank oraz nie stanowią zbioru zamkniętego. Z tego względu zalecamy również korzystanie z innych dobrych praktyk rynkowych oraz systemów.

W celu zabezpieczenia procesów i kompletnego audytu rekomendujemy korzystanie z usług wyspecjalizowanej firmy zajmującej się bezpieczeństwem/cyberbezpieczeństwem w Państwa branży.