

Lista rekomendacji RSP dotyczących działań na rzecz ograniczania transakcji oszukańczych w płatnościach detalicznych w Polsce

I. Rekomendacje w obszarze prawa

1. Rozważenie wprowadzenia rozwiązań prawnych umożliwiających wymianę informacji prawnie chronionych pomiędzy podmiotami z różnych sektorów (bankowego, telekomunikacyjnego, ubezpieczeniowego, niebankowych dostawców usług płatniczych).

2. Rozważenie wprowadzenia rozwiązań prawnych umożliwiających zmianę zasad dostępu przez Policję i Prokuraturę do informacji objętych tajemnicą bankową w szczególnych przypadkach związanych z wykrywaniem i ściganiem przestępczości.

3. Identyfikacja i eliminacja zidentyfikowanych barier prawnych, uniemożliwiających skuteczne przeciwdziałanie oszustwom związanym z przestępczymi platformami internetowymi oferującymi rzekome inwestycje w krypto-aktywa i na rynku FOREX, poprzez wprowadzenie dla banków uprawnień do skutecznego powstrzymywania podejrzanych operacji oraz możliwości pozyskiwania przez banki dodatkowych informacji na potrzeby analizy antyfraudowej, bez uszczerbku dla zachowania prawa do prywatności.

4. Rozważenie dokonania w przepisach prawa lub rekomendacjach KNF zmian mających na celu dodatkową ochronę prawną pracowników obszarów zajmujących się bezpieczeństwem z uwagi na fakt, iż jest to praca często angażująca pracownika do współpracy z organami ścigania, niosąca za sobą konieczność składania zeznań i stawiania się na rozprawach sądowych, obciążona silnym stresem związanym z działaniem pod presją czasu, aby zapobiec skutkom kradzieży pieniędzy czy też z konfrontacją na sali rozpraw z oskarżonymi o przestępstwa na szkodę banków i ich klientów. Taka praca wiąże się z wysokim ryzykiem popełnienia błędu np. pod kątem ryzyka ujawniania tajemnicy zawodowej, bankowej czy złamania zasad RODO.

5. Stworzenie podstawy prawnej (np. w ustawie o Systemie Informacji Finansowej¹) dla wprowadzenia rozwiązania umożliwiającego kontrolę zgodności numeru rachunku odbiorcy płatności z jego danymi osobowymi (imieniem i nazwiskiem) przed dokonaniem transakcji. Takie rozwiązanie pomogłoby uniknąć bardzo wielu

¹ Ustawa jest aktualnie w toku procesu legislacyjnego. Ustawa ta będzie stanowiła podstawę prawną dla utworzenia centralnej bazy rachunków płatniczych. W proponowanych przepisach określono typ informacji o rachunkach, które mają być przekazywane przez podmioty zobligowane do dostarczania informacji o rachunku do SInF (tzw. instytucje zobowiązane). Zakres przekazywanych informacji o rachunku zawiera między innymi: dane identyfikacyjne (w tym imię i nazwisko oraz obywatelstwo) posiadaczy rachunku, pełnomocników do rachunku, beneficjentów rzeczywistych posiadaczy rachunku oraz datę otwarcia i zamknięcia rachunku.

przypadkowych lub wynikających z manipulacji przestępców błędnie skierowanych płatności do nieodpowiedniego właściciela rachunku i zapewniłoby dodatkową ochronę w walce z oszustami.

II. Rekomendacje w obszarze procesów

1. Powszechne wykorzystanie funkcji geoblokowania dla płatności kartowych dokonanych poza UE (np. blokowanie płatności z konkretnych obszarów geograficznych dokonywanych z użyciem paska magnetycznego) i danie możliwości odblokowania takich płatności klientowi, który zgłosi taką potrzebę.
2. Umożliwienie samodzielnego ustawiania limitów dla płatności bez obecności karty (CNP) i udostępnianie ograniczonych limitów ilościowych i kwotowych dla płatności CNP klientom, którzy z takich płatności z dużym prawdopodobieństwem nie będą korzystać.
3. Wprowadzenie na rynku polskim odpowiednika brytyjskiej usługi Confirmation of Payee.
4. Identyfikacja rzeczywistych łańcuchów transakcji przestępczych połączona z blokadą środków i wykrywaniem skompromitowanych rachunków oraz danych osobowych i kontaktowych wykorzystywanych do utylizacji środków pochodzących z przestępstwa.
5. Uwzględnienie w systemach wymiany informacji pomiędzy bankami informacji o transakcjach i zautomatyzowanie ich na tyle, by można było sprawnie blokować wypłaty „na słupa” w innych bankach.
6. Rozwijanie współpracy międzybankowej oraz międzysektorowej z organami ścigania w ramach tworzonych przez finCERT.pl - BCC ZBP grup operacyjnych, w szczególności obejmującej wymianę wrażliwych informacji o konkretnych modus operandi w bezpiecznych kanałach elektronicznych.
7. Szersze współdzielenie najlepszych praktyk w zakresie monitorowania i zapobiegania wyłudzeniom, ukierunkowane na szybką komunikację zidentyfikowanych przypadków do innych uczestników rynku usług płatniczych.
8. Zwiększenie nakładów u dostawców usług płatniczych na podniesienie świadomości użytkownika końcowego - klienta, zwiększenie nakładów na system ochrony i obrony przed zaawansowanymi atakami.
9. Rozpowszechnienie innych niż numer karty płatniczej rozwiązań do płatności w Internecie, np. płatność BLIKiem lub tokenizacja, polegająca na zastąpieniu numeru karty płatniczej unikalnym identyfikatorem cyfrowym.

10. Rozważenie zasadności opracowania dla potrzeb rynku polskiego odpowiednika Fraud Classifier wprowadzonego w USA.

11. Rozważenie wzmocnienia koordynacyjnej roli FinCERT.pl – BCC ZBP jako ISAC w kontekście działań środowiska bankowego i reprezentowania przed UKNF oraz w kontaktach z operatorami telekomunikacyjnymi.

12. Rozważenie możliwości zastosowania w BLIK i innych schematach niekartowych mechanizmów chargeback podobnych jak w schematach kartowych.

13. Rozważenie potrzeby zorganizowania scentralizowanego systemu raportowania transakcji oszukańczych dla metod płatności BLIK oraz przelewów bankowych procesowanych przez operatorów płatności, z dostępem raportujących podmiotów do zagregowanych danych (analogicznie jak zorganizowane to zostało przez Visa TC40 lub Mastercard SAFE).

14. Rozważenie możliwości powstania systemu antyfraudowego na poziomie ogólnokrajowym, w którym mógłby być monitorowany pełen obraz przepływów pieniędzy, informacji i powiązań między obiektami, gdyż nie da się tego zaobserwować na szczeblu poszczególnych banków oraz innych instytucji finansowych.

III. Rekomendacje w obszarze technologii

1. Wprowadzenie zaawansowanej technologii do monitorowania płatności dokonywanych polskimi kartami płatniczymi poza granicami Polski.

2. Stosowanie narzędzi pozwalających wykryć zdalny pulpit wykorzystany w urządzeniu, które inicjuje płatność.

3. Wykorzystanie w procesach, w których dochodzi do inicjowania płatności, technologii pozwalającej na identyfikację urządzenia użytego do płatności (największą synergię zagwarantuje wykorzystanie jednego standardu w ramach sektora bankowego i usług płatniczych przez wiele organizacji).

4. Wprowadzenie uwierzytelnienia wieloskładnikowego wykorzystującego biometrię behawioralną opartą na analizie zachowania użytkownika (biometria behawioralna).

5. Wypracowanie nowych rozwiązań technologicznych umożliwiających szybką i zautomatyzowaną wymianę informacji np. o skompromitowanych: rachunkach bankowych, danych osobowych i kontaktowych, adresach IP ze znacznikami czasu i numerach portów, urządzeń i indeksów biometrii behawioralnej przestępców pomiędzy bankami, przedsiębiorcami z innych sektorów oraz organami ścigania i GIIF.

6. Rozważenie możliwości wdrożenia przez dostawców usług płatniczych mechanizmu uwierzytelniania poczty mailowej DMARC (Domain-based Message Authentication, Reporting and Conformance), mającej na celu zapobieganie fałszowaniu maili i podszywania się pod domeny tych dostawców (phishing, e-mail spoofing).

IV. Rekomendacje w obszarze edukacji

1. Dbanie o świadomość społeczeństwa w zakresie bezpieczeństwa płatności i cyberbezpieczeństwa poprzez różnego rodzaju inicjatywy oraz szeroko zakrojone kampanie edukacyjne i informacyjne, szczególnie kierowane w stronę osób starszych, mające na celu upowszechnianie wiedzy na temat metod socjotechnicznych i manipulacji, których używają oszuści.
2. Wydawanie skierowanych do klientów ostrzeżeń o różnych zagrożeniach i oszustwach, upowszechnianie dobrych praktyk bezpiecznego postępowania klientów oraz przeprowadzanie kampanii edukacyjnych adresowanych do różnych grup odbiorców – z wykorzystaniem środków przekazu popularnych w danej grupie.
3. Przeprowadzanie dla pracowników instytucji finansowych szkoleń podnoszących kompetencje w obszarze bezpieczeństwa płatności i cyberbezpieczeństwa, m.in. w celu wspierania klientów w tym zakresie.
4. Organizowanie dla organów ścigania i wymiaru sprawiedliwości specjalistycznych szkoleń lub warsztatów w obszarze bezpieczeństwa płatności i cyberbezpieczeństwa na bazie realnych studiów przypadku.
5. Przygotowywanie treści edukacyjnych dotyczących bezpieczeństwa płatności i cyberbezpieczeństwa oraz proponowanie ich włączenia w programy właściwych studiów podyplomowych i szkoleń branżowych podmiotom je prowadzącym.
6. Wspieranie edukacji szkolnej i przedszkolnej w zakresie aspektów cyberbezpieczeństwa i zasad bezpieczeństwa związanych z płatnościami, np. poprzez prowadzenie szkoleń dla nauczycieli, opracowywanie i udostępnianie im narzędzi edukacyjnych: scenariuszy lekcji, filmów, gier, aplikacji edukacyjnych itp.