Projekt finansowany w ramach Programu
Leonardo da Vinci
PL/08/LLP-LdV/VETPRO/140103

Projekt wymiany doświadczeń pomiędzy:

Komendą Wojewódzką Policji we Wrocławiu

a

Inspektoratem Głównym Policji Rumuńskiej w Bukareszcie

WYMIANA DOŚWIADCZEŃ W ZAKRESIE PRZESTĘPCZOŚCI W OBIEGU ELEKTRONICZNYMI ŚRODKAMI PŁATNICZYMI

Partnerzy projektu:

Komenda Główna Policji

Komenda Wojewódzka Policji w Bydgoszczy

Szkoła Policji w Katowicach

1. Wstęp

Karty bankowe stanowią nieodłączny element rzeczywistości, a ich posiadanie stało się niemal koniecznością. Należy przy tym pamiętać, że pomimo licznych fizycznych zabezpieczeń oraz podejmowanych przez instytucje bankowe działań mających na celu poprawę bezpieczeństwa, karty nie są wolne od wad, a ich używanie niesie ze sobą pewne ryzyko. Wraz ze wzrostem liczby kart na rynku, pojawiają się coraz to nowe rodzaje dokonywanych przestępstw z wykorzystaniem tego instrumentu płatniczego. O rzeczywistej skali tego problemu świadczy powoływanie specjalnych komórek, zarówno w policji, jak i w bankach, monitorujących wszystkie transakcje dokonywane kartami płatniczymi oraz podejmujących działania prewencyjne w podejrzanych przypadkach. Wraz ze wzrostem liczby kart znajdujących się w obrocie oraz liczby punktów akceptujących płatności kartami, obserwujemy jednocześnie wzrost przestępczości z tym związanej. Rozwój rynku kartowego powoduje coraz bardziej wyrafinowane i zorganizowane działania ze strony grup przestępczych. Przestępstwa dokonywane są na duże kwoty, a sprawcami są inteligentni, posiadający dużą wiedzę i umiejętności młodzi ludzie.

Policja coraz częściej zajmuje się przestępstwami związanymi z nieuprawnionym użyciem plastikowego pieniądza. Choć większość przestępstw związana jest z kradzieżą karty i dokonywaniem zakupów za jej pomocą, to obecnie coraz częściej mają miejsce przestępstwa związane z fałszowaniem kart, czy nawet ich produkcją. Dla wielu może okazać się to szokiem, ale fakty te zdają się zaprzeczać jakoby karta płatnicza była bezpieczną odmianą pieniądza. Powszechne jest przekonanie, że używanie karty jest dużo bezpieczniejsze niż noszenie gotówki. Przyczyna tego stanu rzeczy, leży niestety w niskiej świadomości społecznej, jak łatwo utracić środki pieniężne posiadając kartę bankową. Z jednej strony przyczyniają się do tego reklamy spotykane na każdym kroku, przekonujące nas o olbrzymich zaletach tego produktu, z drugiej zaś strony brak jest rzetelnej i uczciwej informacji ze strony banków, o czyhających niebezpieczeństwach związanych z posiadaniem kart.

2. Przestępstwa kartowe

Wyróżnić można kilka głównych, najczęściej powtarzających się form przestępstw kartowych:

- **Karty zagubione i skradzione (lost, stolen cards)**

Przestępcy wchodzą w posiadanie karty i nie zmieniając danych podszywają się pod autentycznego użytkownika karty, a następnie fałszują podpis korzystając ze wzoru na pasku podpisu.

- **Karty niedoręczone (card not received)**

Działanie przestępcy skupia się na przechwyceniu karty w drodze pocztowej. Zagrożenie tym typem przestępstwa jest bardzo duże, gdyż karty przejęte w drodze od wystawcy do użytkownika długi czas nie są zgłoszone jako utracone i przestępca swobodnie może nimi dysponować bez większego ryzyka, oraz nie są podpisane i fałszerz może nakreślić na pasku dowolny wzór podpisu.

- **Karty otrzymane w oparciu o wniosek z fałszowanymi danymi**

W ujęciu wartościowym stanowią one 70% przestępstw związanych z wykorzystaniem kart płatniczych. Co ważne, na Zachodzie tego rodzaju przestępstwa są bardzo sporadyczne - wynika to z bardzo dobrego zabezpieczenia dokumentów tożsamości przed fałszerstwami. Fałszerz musi przejść całą drogę uzyskania karty płatniczej, co jest dość długotrwałe i ryzykowne, ale otrzymuje oryginalną kartę płatniczą.

- **Fałszerstwa kart (counterfeit)**

Próby fałszowania kart płatniczych są podejmowane od momentu ich powstania i przybierają różnorodne formy. Czasem efekt jest bardzo prymitywny, jednak coraz częściej przybierają formę perfekcyjnych i w pełni profesjonalnych.

- **Karty podrabiane**

Podrabiane karty wykonywane są w całości przez fałszerza w oparciu o oryginalną kartę i autentyczne lub częściowo fikcyjne dane. Źródłem danych autentycznych są np. oryginalne karty lub rachunki i kwity obciążeniowe. Elementy graficzne na kartę nadrukowywane są popularnymi technikami drukarskimi. Profesjonalne grupy przestępcze są w stanie w bardzo krótkim czasie po wejściu w posiadanie karty wykonać jej duplikat. Właściwy użytkownik nawet nie podejrzewa, że jego karta została powielona. Posługują się do tego profesjonalnym i zminiaturyzowanym sprzętem, wykorzystując np. metodę skimmingu. Jest to rodzaj przestępstwa z użyciem kart płatniczych, które polega na tym, że fałszerz kopiuje dane znajdujące się na pasku magnetycznym karty za pomocą specjalnego czytnika elektronicznego. Samo kopiowanie poufnych danych trwa zaledwie kilka sekund.

- **Karty przerabiane**

Przerabianie kart polega na zmianie danych na oryginalnych kartach. Zmieniane są tłoczenia numerów, aby ominąć zastrzeżenia karty, (karta ze zmienioną choćby jedną cyfrą nie figuruje jako karta zastrzeżona), zasięg terytorialny karty (z karty krajowej otrzymuje się międzynarodową), zmieniane są daty ważności karty. Fałszerze termicznie "zaprasowują" oryginalne tłoczenia, tłoczą nowe elementy, ścinają fragmenty cyfr, wykonują "nowe" tłoczenia. Spotyka się również zmiany w obrębie paska z wzorem podpisu. Podpis jest całkowicie lub w części usuwany poprzez działania mechaniczne lub chemiczne. Czasami przestępcy po prostu naklejają pasek z nowym podpisem na pasek oryginalny.

- **Biały plastik (White plastik)**

Na kawałek białego plastiku nanoszone są wytłoczenia z niezbędnymi danymi. Karta taka nie musi posiadać żadnych więcej elementów. Ten typ przestępstwa często wymaga współdziałania przestępcy z osobami obsługującymi terminale POS. Białe karty również ułatwiają przestępcom wypłaty gotówki z bankomatu.

Rys. 1 Biały plastik („White plastic”) (Źródło: materiały własne KWP we Wrocławiu)

- **Fałszerstwa elektroniczne**

Nowoczesna technika pozwala zmienić zawartość paska magnetycznego, co w dobie Internetu, gdzie można znaleźć algorytmy postępowania, nie jest trudne. Co więcej sposób zapisywania informacji na pasku jest określony odpowiednimi normami ISO. Przykładem może tu być taka modyfikacja danych, by terminal rozpoznawał kartę płaską jako embosowaną - czyli nie wymuszającą autoryzacji. Dokonując zmiany zawartości paska magnetycznego, można również zwiększyć limit dostępny na karcie, zmienić datę ważności, a nawet numer karty. Zmiany elektroniczne są czynnościami wykorzystywaniu, zarówno przy podrobieniu, jak i przerobieniu karty.

- **Nielegalne wykorzystanie numeru karty, ryzyko zakupów w Internecie**

Przestępstwa tego rodzaju polegają na nieupoważnionym posługiwaniu się danymi z karty przy zamówieniach telefonicznych, pocztowych czy emailowych (przez Internet). Z danych policyjnych wynika, że proceder sprzedaży numerów kart zatacza coraz szersze kręgi - wykonanie kserokopii z karty na zapleczu np. w restauracji trwa dosłownie chwilę, dlatego nie należy pozwolić, aby w momencie zapłaty karta znikła nam z oczu. Inną metodą zdobycia numerów kart są programy do generowania poprawnych numerów. Programy te są dostępne w Internecie, pomimo usilnych starań blokowania stron zawierających tego typu informacje.

2.1 Skimming

Jedną z coraz powszechniej stosowanych metod przestępczych jest skimming. Polega on na kopiowaniu zawartości paska magnetycznego karty płatniczej bez zgody jej właściciela. Później tak skopiowany pasek jest nanoszony na inną kartę płatniczą, którą przestępcy dokonują zakupów. Oczywiście wszystkie zakupy są dokonywane na rachunek pierwszej skopiowanej karty i obciążają jej właściciela. Inną odmianą tego przestępstwa jest skimming bankomatowy. W jego przypadku podczas wizyty posiadacza karty przy bankomacie przestępcy sczytują zawartość paska magnetycznego oraz próbują na różne sposoby (przy użyciu kamery video lub specjalnej nakładki na klawiaturę) zdobyć kod PIN karty. Jeśli im się to uda, to skopiowaną kartą pobierają pieniądze w innym bankomacie, także na koszt swojej ofiary.

Miniaturowy skaner jest najczęściej nakładany na wlot służący do wprowadzania karty do bankomatu. Podczas wkładania karty do bankomatu pasek magnetyczny zostaje zarejestrowany. Kod PIN przestępcy poznają dzięki miniaturowej kamerze, która rejestruje jego wprowadzenie. Alternatywną metodą poznania kodu PIN jest nałożenie na oryginalną klawiaturę bankomatu jej dokładnie wykonanej kopii. Klient wpisuje PIN nie na klawiaturze oryginalnej, lecz na kopii, która zapamiętuje wprowadzony kod. Nakładka jest wykonana w taki sposób, że naciskając jej przyciski jednocześnie naciskane są oryginalne klawisze maszyny, w związku z tym klient nie dostrzega jakiejkolwiek różnicy w funkcjonowaniu bankomatu.

Co należy podkreślić, wszystkie wspomniane urządzania są instalowane przez przestępców na zewnątrz bankomatu, ponieważ nie mają oni dostępu do jego środka, dlatego klient, przy zachowaniu dużej dozy ostrożności, jest w stanie zauważyć dodatkowe urządzenia dołączone do bankomatu. W takiej sytuacji powinien odstąpić od wypłaty i natychmiast powiadomić bank oraz Policję.

Rys. 2 Nakładka na bankomat zawierająca urządzenie skimmujące umieszczone na wlocie na karty wraz z kamerą skierowaną na klawiaturę (Źródło: materiały własne KWP we Wrocławiu)

Rys. 3 Demontaż nakładki (Źródło: materiały własne KWP we Wrocławiu)

Rys. 4 Bankomat po ściągnięciu nakładki (Źródło: materiały własne KWP we Wrocławiu)

Do kopiowania karty służy małe urządzenie zawierające czytnik kart oraz pamięć pozwalającą na magazynowanie zawartości pasków magnetycznych. Po skończonym dniu przestępcy podłączają je do komputera i kopiują zawartość wszystkich sczytanych pasków magnetycznych. Urządzenie jest na tyle małe, że może zostać ukryte w dłoni. Znane są także przypadki montażu czytników w ladach lub blatach, tak, że do skopiowania karty wystarczało tylko przejechanie kartą w odpowiedni sposób po ich powierzchni.

Rys. 5 Oryginalna klawiatura bankomatu (Źródło: materiały własne KWP we Wrocławiu)

Rys. 6 Nakładka na klawiaturę (Źródło: materiały własne KWP we Wrocławiu)

Rys. 7 Bankomat „czysty” (Źródło: materiały własne KWP we Wrocławiu)

Rys. 8 Bankomat z czytnikiem pasków
(Źródło: http://www.kartyonline.pl/arty.php?id=104&_Powstrzymac_skimming)

Rys. 9 Nakładka na bankomat zawierająca urządzenie skimmujące umieszczone na wlocie na karty wraz z nakładką na klawiaturę (Źródło: Materiały własne KWP we Wrocławiu)

Rys. 10 Nakładka na bankomat zawierająca urządzenie skimmujące umieszczone na wlocie na karty (Źródło: Materiały własne KWP we Wrocławiu)

Czytniki kart i wszystkie urządzenia do kopiowania kart można kupić bez najmniejszych problemów w Internecie. Koszt takiego urządzenia nie przekracza 2000 zł. Jest to niewielka suma w porównaniu do zysków z ewentualnej przestępczej działalności.

Szczególnie często skimming zdarza się w barach, restauracjach i na stacjach benzynowych oraz wszędzie tam gdzie, karta znika choćby na chwile z pola widzenia klienta. Karta jest kopiowana przez sprzedawcę, który współpracuje z przestępcami lub sam jest przestępcą.

Łatwość, z jaką można uzyskać środki finansowe powoduje, że skimming staje się przestępstwem powszechnym zarówno w USA, jak i w całej Europie. Policja zna liczne międzynarodowe grupy przestępcze, które działają na terytorium kilku państw, w jednym kopiują karty, w innym zaś realizują zyski z tego procederu. Bardzo pomocny w tej działalności jest Internet, który pozwala przesyłać zawartość paska magnetycznego karty w ciągu kilku sekund w dowolne miejsce na ziemi.

Zawartość pasków magnetycznych przestępcy nanoszą na inne karty płatnicze. Jeśli z daną grupą współpracuje sprzedawca, to zawartość paska zostaje naniesiona na czystą białą kartą (nazywaną "*white plastic*"). Taką kartą przestępcy dokonują zakupów w terminalu współpracującego z nimi sprzedawcy.

Jeśli grupa chce dokonywać zakupów w innych punktach handlowych, to musi nagrać pasek magnetyczny na oryginalna lub podobną do oryginału kartę, tak by sprzedawca nie zorientował się w oszustwie. W tym celu przestępcy wykorzystują skradzione oryginalne karty płatnicze lub też starają się, bardziej lub mniej udolnie, podrabiać karty.

Jeśli przestępcy wykorzystują do zakupów oryginalną kartę danego banku, to fałszerstwo można w łatwy sposób wychwycić sprawdzając czy numer karty na wyciągu z terminala jest zgodny z numerem znajdującym się na karcie. Jeśli numery te się różnią, oznacza to, że karta została sfabrykowana przez przestępców poprzez nałożenie innego paska magnetycznego.

Aby natomiast wychwycić podrobioną kartę sprzedawca musi zwracać uwagę na jakość jej wykonania oraz na zabezpieczenia. Powinien w pierwszym rzędzie zwrócić uwagę na kolorystkę karty, jego podejrzenia powinny wzbudzić wszystkie wyblakłe kolory, niedokładności w naniesieniu barw lub przebarwienia. W dalszej kolejności należy sprawdzić hologram organizacji płatniczej, mikrodruk oraz nadruki na pasku podpisu z tyłu karty.

W przypadku kart wypukłych (embosowanych) powinno się zwracając także uwagę na wytłoczone miniaturowe znaki organizacji Visa lub MasterCard, które tylko pozornie wydają się łatwe do podrobienia. Sprzedawca w razie powzięcia podejrzeń powinien zatrzymać kartę i powiadomić o zaistniałym fakcie agenta rozliczeniowego oraz Policję.

Największe straty spowodowane skimmingiem ponoszą banki, choć czasem jego koszty bywają także przerzucane na klienta. Skimming ma bowiem postać przestępstwa dokonywanego seriami, tzn. przestępcy w tym samym miejscu dokonują skanowania większej liczby kart. W ten sposób klient, którego karta została zeskanowana wraz z innymi kartami, ma szansę udowodnić, że doszło do przestępstwa. W przypadku, gdy mu się to nie uda, to bank może uznać go za oszusta, który próbuje wyłudzić z banku pieniądze.

Wiele zależy także od tego, gdzie przestępcy dokonują zakupów zeskanowanymi kartami. Jeśli robią to za granicą, szczególnie w Rosji, na Ukrainie lub krajach azjatyckich, to łatwej w takiej sytuacji przekonać bank, że padło się ofiarą skimmingu.

Dotychczas w nagłaśnianych przez media przypadkach skimmingu, banki zawsze brały na siebie odpowiedzialność za te przestępcze transakcje. Trudno jednak powiedzieć, jak banki zachowują się w sytuacjach, gdy mają tylko jednego poszkodowanego. Tym bardziej, że banki raczej nie wymieniają się informacjami o tego rodzaju reklamacjach, jest im zatem trudno stwierdzić, czy w danej sytuacji doszło do skimmingu, czy też nie.

Występowanie skimmingu jest efektem stosowania na kartach płatniczych przestarzałej technologii paska magnetycznego. Pełne jego wyeliminowanie nastąpi dopiero, gdy z kart znikną paski i w pełni zastąpią je mikroprocesory. Proces wprowadzania kart z chipem już trwa, choć w różnych krajach jego szybkość jest różna. Polska pozostaje w tym procesie, w tyle za najważniejszymi rynkami Europy.

Pierwsze poważne akcje wydawania kart z chipem rozpoczęły się w naszym kraju w 2005 roku. Początkowo jednak wszystkie wydawane karty zawierały zarówno chip, jak i pasek magnetyczny (karty hybrydowe). Ma to umożliwić stopniowe przejście od kart magnetycznych do chipowych, lecz jednocześnie ułatwia życie przestępcom, którzy wciąż będą mogli kopiować paski magnetyczne i w terminalach, które nie obsługują kart chipowych, wykorzystywać sklonowane karty.

Wydaje się więc, że na pełne wyeliminowanie skimmingu potrzeba jeszcze co najmniej kilku, jeśli nie kilkunastu lat. W tym czasie będziemy musieli żyć, ze świadomością, że nasze karty mogą zostać skopiowane i wykorzystane przez przestępców. Dlatego właśnie musimy zacząć aktywnie walczyć ze skimmingiem, by nie przerodził się on w plagę, nad którą nie można zapanować.

3. Przestępstwa komputerowe

Pojęciem **przestępczości komputerowej** określamy wszelkie rodzaje przestępstw, do popełnienia, których użyto komputera, Internetu lub sieci komputerowych. Często nazywamy ją cyberprzestępczością. Komputery oraz sieci komputerowe mogą uczestniczyć w przestępstwie na kilka sposobów:

- komputer lub sieć mogą być narzędziem przestępstwa (zostaną użyte do jego popełnienia)

- komputer lub sieć mogą być celem przestępstwa (ofiarą)

- komputer lub sieć mogą być użyte do zadań dodatkowych związanych z popełnieniem przestępstwa (na przykład do przechowywania danych o nielegalnych działaniach).

W polskim prawie zdefiniowane są przestępstwa z użyciem komputerów, nie ma jednak oficjalnej definicji cyberprzestępstwa. Taką definicję wypracował X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców, i tak:

1) **Cyberprzestępstwo** w wąskim sensie (przestępstwo komputerowe) Wszelkie nielegalne działanie, wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych.
2) **Cyberprzestępstwo** w szerokim sensie (przestępstwo dotyczące komputerów) wszelkie nielegalne działanie, popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi

nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych.

Oczywistym jest fakt, że w jednym kraju pewne działanie uznane za nielegalne w innym może być dozwolone, ma to zwłaszcza ogromne znaczenie w najczęstszej w Internecie sytuacji, kiedy sprawcę dzielą tysiące kilometrów od ofiary.

Przestępstwa komputerowe to wszelkie zachowania przestępcze związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszaniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer.

3.1 Przestępstwa przeciw ochronie informacji

Regulacje dotyczące przestępstw przeciw ochronie informacji mają swoje umocowanie w Kodeksie Karnym.

Rodzaje przestępstw przeciw ochronie informacji:

- **hacking komputerowy** – to takie działanie sprawcy, który bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie.
- **nielegalny podsłuch i inwigilacja przy użyciu urządzeń technicznych** - polega na zakładaniu lub posługiwaniu się urządzeniami podsłuchowymi, wizualnymi albo innymi urządzeniami specjalnymi w celu uzyskania informacji, do której nie jest się uprawnionym. Regulację tą stosuje się przede wszystkim w sytuacji podsłuchiwania naszych rozmów telefonicznych, czy też rozmów codziennych np. w pomieszczeniu. Przykładowo można podać, jakie urządzenia ustawodawca miał na myśli, mówiąc o „innych urządzeniach specjalnych”. Mogą to być: specjalne mikrofony np. mikrofony kierunkowe (urządzenia o bardzo wysokiej czułości), kamery, urządzenia podłączane do kabla telefonicznego w celu zbierania danych itp.

- **naruszenie integralności komputerowego zapisu informacji** - chodzi tutaj o naruszenie integralności komputerowego zapisu informacji, które może nastąpić wskutek bezprawnego niszczenia, uszkadzania, usuwania lub zmiany zapisu istotnej informacji albo udaremniania czy utrudniania osobie uprawnionej zapoznanie się z nią.
- **sabotaż komputerowy** – polega na doprowadzeniu do sparaliżowania systemu komputerowego, zakłócaniu lub paraliżowaniu funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli. Sabotaż komputerowy może wystąpić również w formie niszczenia lub wymiany nośnika informacji, niszczenia albo uszkodzenia urządzeń służących do automatycznego przetwarzania, gromadzenia bądź przesyłania informacji.

3.2 Przestępstwa przeciw wiarygodności dokumentów

Rodzaje tego typu przestępstw:

- **fałszerstwo dokumentu** dokonane przez osobę, która podrabia lub przerabia dokument lub takiego dokumentu używa, jako autentycznego. Jest to fałszerstwo komputerowego zapisu informacji stanowiącego dokument.
- **zniszczenie, uszkodzenie, ukrycie lub usunięcie dokumentu -** polega na niszczeniu, uszkadzaniu, ukryciu lub usunięciu dokumentu przez osobę, która nie ma prawa nim rozporządzać.

3.3 Przestępstwa przeciwko mieniu

Rodzaje tego typu przestępstw:

- **Kradzież programu komputerowego** ma miejsce wtedy, gdy przestępca w jakikolwiek sposób zdobywa program komputerowy (np. kopiowanie, zabranie dyskietki lub innego nośnika) nie mając na to wyraźnej zgody (np. licencji) osoby uprawnionej według prawa autorskiego (np. twórcy programu).
- **Paserstwo komputerowe**

  Paserstwo umyślne ma miejsce wtedy, gdy osoba postronna nabywa program komputerowy wiedząc, że program ten został np. skradziony lub bezprawnie skopiowany (np. właściciel sklepu wiedząc, iż oferowany mu

program komputerowy został skradziony, zgadza się sprzedać go w swoim sklepie lub pomaga w ukryciu tego programu, albo przyjmuje go - np. na przechowanie).

Paserstwo nieumyślne zachodzi w przypadkach takich jak: nabycie, pomoc w zbyciu lub ukryciu oraz przyjęcie programu komputerowego - jeśli przestępca jedynie powinien lub może przypuszczać, że program został np. ukradziony (przykładowo osoba postronna nabywa na giełdzie komputerowej program, który oferowany jest po okazyjnie niskiej cenie).

- **Oszustwa komputerowe -** polegają na takim działaniu sprawcy, który w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji.

  Szczególnym rodzajem oszustwa komputerowego jest **„phishing”**, czyli przestępstwo związane z kradzieżą (przejęciem) tożsamości – najczęściej związane z włamaniem na konta bankowe.

  „Phishing” polega na tworzeniu oszukańczych wiadomości e-mail i witryn WWW, które wyglądają identycznie, jak serwisy internetowe znanych firm, aby skłonić klientów tych firm do podania swoich danych osobowych, numeru karty kredytowej lub informacji o elektronicznym rachunku bankowym – kodów i haseł potrzebnych do zalogowania i autoryzacji transakcji.

  „Phishing” obejmuje bezprawne pozyskiwanie:

  - danych kart płatniczych wraz z przyporządkowanymi im kodami („PIN” lub „CVV2”/„CVC2”),

  - kodów autoryzacyjnych i haseł do elektronicznych rachunków bankowych.

  Dane te są najczęściej pozyskiwane przy wykorzystaniu:

  - rozsyłanych fałszywych e-maili z odnośnikami – linkami – do spreparowanej strony WWW e-banku, serwisu płatności lub serwisu aukcyjnego,

  - złośliwego oprogramowania komputerowego.

  Pozyskane w ten sposób dane wykorzystywane są do oszukańczych transakcji internetowych lub kradzieży pieniędzy z rachunków bankowych. W Polsce pierwsze przypadki phishingu zanotowano w 2001 roku. Ich liczba wzrasta jednak z roku na rok. Według nieoficjalnych statystyk, na całym

świecie codziennie likwiduje się do 10 stron internetowych podszywających się pod strony banków.

Narzędzia wykorzystywane przez sprawców do pozyskiwania danych to zazwyczaj:

- programy szpiegujące, np. typu „trojan”,
- fałszywe strony WWW wirtualnych banków,
- strony WWW z zamieszczonymi plikami do pobrania, zawierające programy typu „keylogger”,
- fałszywe e-maile pochodzące rzekomo od banków, systemów czy serwisów płatniczych bądź aukcyjnych, zawierające odnośniki do fałszywych stron internetowych.

4. Sposoby ochrony przed przestępczością

4.1 Bezpieczeństwo transakcji bankowych w Internecie

Poniżej przedstawiono informacje o bezpiecznym wykorzystaniu kart płatniczych oraz dokonywaniu transakcji w sklepach internetowych oraz korzystaniu z dostępu do pieniędzy za pośrednictwem zdalnych kanałów dostępu - Internetu, telefonu.

1. Żaden bank nigdy nie wysyła do swoich klientów pytań dotyczących haseł lub innych poufnych danych ani próśb o ich aktualizację.

Banki nigdy nie podają w przesyłanych wiadomościach linków do stron transakcyjnych. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie należy odpowiadać na nie, gdyż przekazuje się tym samym swoje poufne dane. Bezzwłocznie należy skontaktować się ze Bankiem i poinformować o zdarzeniu.

2. Należy sprawdzić na stronie Banku, jakie zabezpieczenia stosowane są w serwisie internetowym.

Przy każdym logowaniu bezwzględnie należy stosować się do zasad bezpieczeństwa tam opublikowanych. W przypadku pojawienia się jakichkolwiek nieprawidłowości natychmiast należy skontaktować się z pracownikiem Banku.

3. Komputer lub telefon komórkowy podłączony do Internetu musi mieć zainstalowany program antywirusowy i musi on być na bieżąco aktualizowany.
Niezbędna jest również aktywacja istotnych modułów w pakiecie ochronnym takich jak monitor antywirusowy, skaner poczty czy firewall. Częstym błędem jest wyłączanie wspomnianych modułów w celu redukcji obciążenia systemu.

4. Należy dokonywać płatności internetowych tylko z wykorzystaniem „pewnych komputerów".
Nie należy dokonywać płatności internetowych z komputerów znajdujących się w miejscach publicznych np. w kawiarenkach internetowych lub na uczelni.

5. Należy skontaktować się ze swoim dostawcą Internetu w celu upewnienia się, że korzysta on z bezpiecznych kanałów dystrybucji tej usługi.
Należy zwracać szczególną uwagę na jakość i bezpieczeństwo usług internetowych dostarczanych przez dostawcę. W przypadku wątpliwości w tym zakresie zawsze jest możliwość zapytania się dostawcy o jakość bezpieczeństwa oferowanego przez niego.

6. Należy instalować na swoim komputerze tylko legalne oprogramowanie.
Programy niewiadomego pochodzenia, w tym ściągane za pośrednictwem programów typu Peer-to-Peer (P2P) mogą być przygotowane przez hakerów i zawierać wirusy lub inne szkodliwe oprogramowanie.

7. Zaleca się okresowe wykonanie skanowania komputera, w szczególności przed wejściem na stronę internetową banku i wykonaniem jakiejkolwiek transakcji.
Większość programów antywirusowych przy włączonym monitorze antywirusowym ma detekcję (wykrywalność) taką samą jak skaner antywirusowy i nie ma konieczności skanowania komputera. Jest jednak część programów, których detekcja

monitora antywirusowego jest niższa aniżeli skanera, powoduje to jednak lukę w systemie bezpieczeństwa.

8. Należy aktualizować system operacyjny i istotne dla jego funkcjonowania aplikacje np. przeglądarki internetowe.

Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych i aplikacji publikują stosowne „łaty", których celem jest usuwanie podatności ich produktów na ataki przeprowadzane za pośrednictwem znalezionych luk.

9. Nie należy otwierać wiadomości i dołączonych do nich załączników nieznanego pochodzenia.

Często załączniki takie zawierają wirusy lub inne oprogramowanie, które pozwalają na „szpiegowanie" działań użytkownika.

10. Należy unikać stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje.

Szczególnie niebezpieczne mogą być strony internetowe zawierające treści pornograficzne. Ponadto z pozoru niewinne strony zawierające programy typu „freeware" również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często dekompilują je uzupełniając o złośliwy kod.

4.2 Zasady dotyczące płatności z internetowego konta bankowego

1. Po zalogowaniu do systemu transakcyjnego nie należy odchodzić od komputera, a po zakończeniu pracy należy wylogować się i zamknąć przeglądarkę.

2. Jeśli przy logowaniu pojawią się nietypowe komunikaty lub prośby o podanie danych osobowych lub dodatkowe pola z pytaniem o hasła do autoryzacji, natychmiast należy zgłosić problem do swojego Banku.

3. Nie należy wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w przychodzących mailach (Phishing).

Należy używać do tego celu adresu podanego przez Bank, z którym podpisano umowę o otwarcie i prowadzenia rachunku bankowego. Nie jest również wskazane wykorzystywanie mechanizmu „Zakładek" (Firefox) lub „adresów Ulubionych" (Internet Explorer), gdyż istnieją szkodliwe obiekty, które potrafią modyfikować zachowane tam adresy.

4. Nigdy nie należy używać wyszukiwarek internetowych do znalezienia strony logowania Banku.

Wyszukane w nich linki mogą prowadzić do fałszywych stron lub stron zawierających wirusy.

5. Przed zalogowaniem należy sprawdzić, czy połączenie z bankiem jest szyfrowane.

Jeśli tak, adres witryny powinien rozpoczynać się od https://, a w dole ekranu przeglądarki www powinien pojawić się symbol zamkniętej kłódki, to oznacza, że informacje są przesyłane z wykorzystaniem 128-bitowych algorytmów szyfrujących. Brak kłódki lub otwarta kłódka oznacza brak szyfrowania, czyli, że dane są transmitowane przez Internet tekstem jawnym, co naraża użytkownika na ogromne niebezpieczeństwo.

6. Należy sprawdzać prawidłowość certyfikatu.

Zanim zostanie wpisany identyfikator bądź login i hasło, należy sprawdzić certyfikat witryny (kliknięcie w kłódkę), czyli przede wszystkim jego datę ważności i dla kogo został wystawiony. Jeśli certyfikat utracił ważność lub nie można go zweryfikować należy zrezygnować z połączenia.

7. Nigdy nie udostępniamy osobom trzecim identyfikatora ani hasła dostępu.

Identyfikator jest poufnym numerem nadawanym przez Bank, nie można go zmienić.

8. Nie należy zapisywać nigdzie haseł służących do logowania i pamięta o ich regularnej zmianie.

Idealnym rozwiązaniem jest zmienianie haseł raz w miesiącu, ale o ile system tego nie wymusi należy zmieniać je przynajmniej raz na dwa miesiące używając kombinacji dużych i małych liter oraz cyfr.

9. Należy sprawdzać datę ostatniego poprawnego oraz niepoprawnego logowania do systemu.

10. Zaleca się korzystanie z infolinii udostępnionej przez bank.

Każdy klient zawsze ma prawo skorzystać z infolinii swojego banku, jeśli wystąpią wątpliwości w zakresie bezpiecznych transakcji bankowych wykonywanych za pośrednictwem internetu.

4.3 Zasady bezpiecznego korzystania z kart płatniczych

1. O ile to możliwe, należy korzystać ze znanych bankomatów. Będzie wtedy łatwiej zauważyć ewentualne zmiany, jakie zaszły w wyglądzie urządzania. W przypadku zauważenia podejrzanych zmian, należy poinformować bank lub Policję.

2. Należy dokładnie sprawdzać, czy do bankomatu nie są dołączone od zewnątrz żadne urządzenia. Jeśli zostanie zauważony podejrzanie wyglądający element, należy zrezygnować z wypłaty i zgłoś obawy do banku.

3. Dokładnie należy przyglądać się otoczeniu bankomatu, a w przypadku zauważenia czegoś podejrzanego, należy zrezygnować z wypłaty.

4. Nigdy nie należy korzystać przy bankomacie z pomocy nieznanych osób.

5. Kiedy wprowadza się kod PIN, należy zawsze zasłaniać klawiaturę ręką, i to w taki sposób by nie można było podejrzeć kodu z żadnej strony. Należy nauczyć się wprowadzać PIN automatycznie, bez patrzenia na klawisze numeryczne. Jest wielce prawdopodobne, że jeśli właściciel karty widzi wprowadzany przez siebie PIN, mogą go też zobaczyć przestępcy.

6. Kiedy płaci się kartą w sklepie, nigdy nie należy „trać jej z oczu”.

7. Jeśli dla potwierdzenia transakcji w sklepie wymagane jest wprowadzenie kodu PIN, należy zrobić to tak, by nikt, łącznie z właścicielem karty, nie widział wpisywanego kodu.

8. Należy zwracać uwagę na to, co sprzedawca robi z kartą. Powinien przejechać jej paskiem magnetycznym przez czytnik w terminalu POS. Później nie powinien już wprowadzać ani zbliżać karty do innych urządzeń.

9. Należy kontrolować na bieżąco stan konta, jeśli zauważy się transakcje, których nie dokonano, natychmiast należy poinformować o tym bank i zastrzec kartę.

5. Wymiana doświadczeń – Bukareszt (Rumunia) 07-13.09.2008r.

W ramach Programu Leonardo da Vinci 10-osobowa grupa policjantów zajmujących się zwalczaniem przestępczości z użyciem elektronicznych środków płatniczych, uczestniczyła w wymianie doświadczeń w Inspektoracie Głównym Policji Rumuńskiej w Bukareszcie. Celem projektu było zapoznanie się z nowymi technikami i rozwiązaniami w zakresie przestępczości kartowej, stosowanymi przez partnera

rumuńskiego.

Strona rumuńska wskazała, że obserwuje wzrost cyberprzestępczości. Zauważalna jest wyraźna migracja zorganizowanych grup przestępczych popełniających do tej pory pospolite przestępstwa kryminalne w kierunku cyberprzestępczości. Przykładowo policja rumuńska odnotowuje obecnie 3 – 4 przypadki miesięcznie tzw. „phishingu", czyli przestępstwa związanego z kradzieżą (przejęciem) tożsamości – najczęściej związanych z włamaniem na konta bankowe, gdy jeszcze do niedawna taka ilość miała miejsce na przełomie całego roku. Podobnie jest w przypadku przestępstw dotyczących elektronicznych instrumentów płatniczych, a w szczególności zjawiska „skimmingu", czyli kopiowania zawartości pasków magnetycznych oraz rejestracji numeru PIN, przy użyciu specjalistycznych urządzeń montowanych na bankomatach lub w terminalach POS, a następnie nanoszenia pozyskanych danych na fałszywe karty i realizacji przy ich pomocy wypłat lub zakupów w sklepach internetowych. Do niedawna notowano na terenie Rumunii 10 przypadków rocznie, a obecnie 3-4 przypadki miesięcznie. Zwalczanie przestępczości kartowej odbywa się w ramach komórek zwalczających cyberprzestępczość.

Policja rumuńska ma świadomość, że jej obywatele popełniają przestępstwa przy użyciu elektronicznych instrumentów płatniczych na terenie całej Europy. Sprzyja temu przystąpienie tego kraju do Unii Europejskiej, swoboda w przemieszczaniu się, oraz podobnie jak w Polsce, duża migracja zarobkowa obywateli Rumunii. Uczestnikom wymiany przedstawiono mapę obszaru Rumunii z uwzględnieniem podziału na regiony oraz wskazaniem miejsc najczęstszego popełniania cyberprzestępstw, jak i przestępstw kartowych. Wynikało z niej, że najczęściej dochodzi do tego rodzaju przestępstw w regionach takich miast jak: Costanca, Bacau, Jassi.

Wśród rozwiązań zastosowanych przez partnera rumuńskiego uczestnicy wymiany najlepiej ocenili przeprowadzoną reformę instytucji państwowych. Na jej mocy instytucje takie jak sądy, prokuratury oraz jednostki policji zostały wyposażone w tę samą strukturę, nazewnictwo oraz zakres działania.

W przypadku cyberprzestępczości na poziomie Inspektoratu Głównego Policji Rumuńskiej istnieje Departament do Walki z Cyberprzestępczością. Departament ten

ma swoje odpowiedniki w prokuraturze, jak i w sądzie. Ten sposób podziału został zachowany również w jednostkach podległych tj. w każdej z 41 rumuńskich komend regionalnych istnieją wydziały zwalczające cyberprzestępczość i taki podział stosowany jest, aż do najmniejszej jednostki organizacyjnej policji. Policjanci rumuńscy w rozmowach kuluarowych podkreślali, że po początkowych problemach związanych z wdrożeniem przedmiotowego podziału, obecnie zaczyna to coraz lepiej funkcjonować i sprawdzać się. Zwłaszcza w przypadku cyberprzestępstw ma to swoje uzasadnienie, gdyż skomplikowany sposób działania sprawców tych przestępstw wykorzystujących często zaawansowane, nowoczesne technologie wymaga specjalistycznej wiedzy, zarówno od policjantów prowadzących proces wykrywczy, jak i współpracujących z nimi prokuratorem, a w późniejszym etapie również od sędziego. Umożliwia to również właściwą koordynację podejmowanych działań oraz wysoce ułatwia prowadzone, wspólnie z prokuraturą, czynności, a także umożliwia realne podniesienie poziomu wykonywanych zadań służbowych.

Uczestnicy wymiany doświadczeń jednogłośnie stwierdzili, że tego typu reforma byłaby doskonałym rozwiązaniem i w Polsce. Bardzo przyspieszyłaby cały proces formalny przy tego typu przestępstwach, gdyż dana sprawa mogłaby zostać przyporządkowana na przykład w prokuraturze osobie znającej zagadnienie cyberprzestępczości, a nie jak dotychczas trafiałaby do przypadkowej osoby. Prokurator nie potrzebowałby czasu na analizę zleconej mu sprawy od zapoznania się z problematyką cyberprzestępczości, gdyż byłby w tej kwestii biegłą osobą. Tym samym decyzja w danej sprawie byłaby wydawana dużo szybciej, wpływając korzystnie na efektywność pracy Policji oraz na wzrost poczucia bezpieczeństwa obywateli.

Wymiana doświadczeń była także dobrą okazją do porównania zakresu prawodawstwa w materii przestępczości kartowej. W tym przypadku partner rumuński odnalazł ciekawe i efektywne rozwiązania w prawodawstwie polskim.

W jednej z prezentacji dotyczącej cyberprzestępczości strona polska omówiła szczegółowo uprawnienia wynikające z art. 20c. polskiej ustawy o policji, prawa telekomunikacyjnego, ustawy o świadczeniu usług drogą elektroniczną oraz kodeksu postępowania karnego.

W polskiej ustawie o policji zawarto szereg uprawnień wspomagających podejmowane przez funkcjonariuszy działania wykrywcze, w szczególności dotyczące możliwości uzyskania:

-danych identyfikujących abonenta;

-danych identyfikujących zakończenie sieci lub urządzeń telekomunikacyjnych, między którymi wykonano połączenie;

-danych dotyczących uzyskania lub próby uzyskania połączenia między określonymi urządzeniami telekomunikacyjnymi lub zakończeniami sieci;

-danych dotyczących okoliczności i rodzaju wykonywanego połączenia.

Ujawnienie danych, o których mowa wyżej, następuje na:

-pisemny wniosek Komendanta Głównego Policji lub Komendanta Wojewódzkiego Policji,

-ustne żądanie policjanta posiadającego pisemne upoważnienie do występowania o przedmiotowe dane.

Zauważono, po wysłuchaniu szczegółowej prezentacji na temat ustawodawstwa rumuńskiego, że tamtejsza policja posiada bardziej restrykcyjne uprawnienia w tym zakresie, mianowicie wszelkie czynności odbywają się poprzez prokuratora, do którego wnioskuje się o wydanie żądania ujawnienia danych, opisując i uzasadniając potrzebę ich uzyskania.

Znaczne różnice, również ocenione jako dające szersze pole funkcjonalności dla podejmowanych działań, stwierdzono w zapisach kodeksu postępowania karnego. Dyspozycja art. 220 k.p.k. określająca przesłanki przeszukania mówi, że w wypadkach nie cierpiących zwłoki, jeżeli postanowienie sądu lub prokuratora nie mogło zostać wydane, organ dokonujący przeszukania okazuje nakaz kierownika swojej jednostki lub legitymację służbową, a następnie zwraca się niezwłocznie do sądu lub prokuratora o zatwierdzenie przeszukania. Policjanci rumuńscy bardzo pozytywnie ocenili taką możliwość, wskazując, że bardzo często właśnie brak możliwości podjęcia natychmiastowych działań i potrzeba uzyskania stosownej dokumentacji stanowi samoistną przeszkodę w prowadzeniu efektywnych działań, gdy następuje dynamiczna zmiana bądź nieoczekiwany rozwój sytuacji operacyjnej.

W przypadku postępowań przygotowawczych prowadzonych na terenie Rumunii wszelkie czynności wykonywane są również na polecenie prokuratura. W przypadku cyfrowych dowodów, w tym komputerów lub dysków twardych przedstawiono uczestnikom wymiany doświadczeń sposób ich zabezpieczenia, a następnie poddania analizie. Zabezpieczony przez policję sprzęt komputerowy jest pakowany w worki, a następnie wraz ze specjalną metryczką plombowany i przekazywany do badań. Badanie polega na wykonaniu kopii dysku twardego za

pomocą sprzętowego „blockera zapisu”, którą to dopiero poddaje się analizie. Czynności te wykonywane są po uprzednim powiadomieniu adwokata podejrzanego, w jego obecności oraz w obecności dwóch postronnych świadków. Wyniki analizy przedstawiane są sądowi. Czynności procesowe takie, jak przeszukanie mieszkania również odbywają się w obecności osoby, której ona dotyczy oraz dwóch postronnych świadków. Do analizy wykorzystywane są najnowsze wersje oprogramowania śledczego.

W zakresie informatyki śledczej stwierdzono, że obie instytucje pracują na identycznym oprogramowaniu tzw. „forensic software” – przeznaczonym do pracy z cyfrowymi dowodami rzeczowymi – zatwierdzonym przez międzynarodowy wymiar sprawiedliwości. W ramach tej dziedziny policja ma możliwość przeprowadzenia następujących działań:

a) badanie zawartości dysków twardych w kierunku:

- ujawniania, pozostających w zainteresowaniu postępowań przygotowawczych, danych stanowiących materiał dowodowy;
- analizy korespondencji e-mail zapisanej w pamięci komputera;
- analizy korespondencji w komunikatorach, prowadzonej przez użytkownika komputera;
- analiza historii odwiedzanych stron internetowych;
- wyszukania słów kluczowych i wiązania z nimi określonych typów danych;

b) odzyskiwanie usuniętych danych z nośników danych cyfrowych;

c) analiza pamięci telefonów komórkowych, organizerów osobistych PDA, tzw. „playerów” multimedialnych;

d) analiza zawartości płyt CD i DVD, pamięci masowych USB.

Godną przeniesienia na grunt polski jest policyjna baza danych, która opiera się na bazie ewidencji ludności. W związku z faktem, iż obywatele rumuńscy w wieku 14 lat uzyskują dokument tożsamości, istnieje możliwość stworzenia bazy danych tych obywateli od 14 roku życia. W bazie, obok danych osobowych, znajdują się także zdjęcia, a aktualizacja wizerunku osoby następuje co 10 lat. Dostęp do tej bazy w znacznym stopniu ułatwia Policji typowanie, ustalanie i identyfikowanie osób. Taka baza danych zwiększa efektywność pracy Policji, gdyż jak statystyki wskazują, że coraz młodsze osoby popełniają przestępstwa na szeroką skalę, a tego typu baza danych znacząco ułatwia ich weryfikację.

Strona rumuńska dużą wagę przykłada do współpracy międzynarodowej podkreślając, że ma to szczególne znaczenie w przypadku cyberprzestępstw, które coraz częściej mają charakter transgraniczny. Wskazano na bardzo dobrą współpracę z Federalnym Biurem Śledczym Stanów Zjednoczonych, przy udziale którego zrealizowano szereg spraw dotyczących cyberprzestępstw. Dzięki procesowi

licznych szkoleń, w tym z udziałem FBI, oraz zmodernizowanej strukturze organizacyjnej policja rumuńska ma w ostatnim czasie coraz więcej sukcesów.

W przypadku zwalczania cyberprzestępczości na uwagę zasługuje utworzenie przez Policję rumuńską, we współpracy ze stroną francuską, strony internetowej www.efrauda.ro, która ma wesprzeć zwalczanie tego zjawiska. Przede wszystkim ma za zadanie uświadamianie społeczeństwa rumuńskiego, co do zagrożeń dotyczących cyberprzestępczości. Na stronie tej oprócz informacji o sposobach działania sprawców, jak i ostrzeżeń, znaleźć można przepisy prawne regulujące zwalczanie tej przestępczości. Ponadto za jej pomocą można przekazać informację lub zgłosić każdy przypadek cyberprzestępstwa. Istnienie tej strony ma również na celu realizację zadań policji rumuńskiej, w zwalczaniu jakiejkolwiek przestępczości, której podstawą jest dobra komunikacja i przepływ informacji pomiędzy obywatelem a policją.

W lipcu 2008 Inspektorat Główny Policji w Bukareszcie wdrożył do realizacji program TRIDENT. Ideą projektu jest reorganizacja pracy służb odpowiedzialnych za przestępczość transgraniczną (przemyt narkotyków, broni, handel żywym towarem, przewóz cudzoziemców spoza Strefy Schengen) w celu skuteczniejszego ujawniania i zwalczania tego rodzaju przestępczości. W tym celu powołano 3 grupy robocze, składające się z funkcjonariuszy Policji, Straży Granicznej i służb celnych. Grupy pracują na granicy rumuńsko-ukraińskiej, rumuńsko-bułgarskiej i na lotnisku w

Bukareszcie. Każdą z grup kieruje funkcjonariusz innej służby. Każda grupa podzielona jest na analityków i zespół realizacyjny. To analitycy (funkcjonariusz graniczny, celnik i policjant) typują przejście graniczne, pojazd oraz towar, który może pochodzić z przestępstwa lub jego posiadanie jest zabronione. W odpowiednim momencie zespół realizacyjny podejmuje odpowiednie działania. Zaledwie w okresie dwóch miesięcy dzięki programowi TRIDENT wykryto kilka poważnych prób przemytu narkotyków oraz usiłowania przewiezienia cudzoziemców na teren Unii Europejskiej.

Strona rumuńska zorganizowała uczestnikom wymiany czas po odbytych zajęciach. Policjanci polscy wspólnie z rumuńskimi spędzali popołudnia na zwiedzaniu zabytków miasta i rozmowach kuluarowych. Był to kolejny element programu, podczas którego uczestnicy mogli w dalszym ciągu wymieniać doświadczenia i poglądy. Uczestnicy wymiany wskazali na jedną główną cechę, która charakteryzowała Bukareszt – miasto można podzielić na dwie części – jedną zadbaną z pięknymi zabytkami, drugą natomiast ubogą i zaniedbaną.

Po zakończeniu wymiany doświadczeń uczestnicy otrzymali certyfikat z ramienia Inspektoratu Generalnego Policji Rumuńskiej w Bukareszcie.

Efektem projektu jest zdobycie przez uczestników nowych doświadczeń, nawiązanie bliższych kontaktów umożliwiających nawiązanie przyszłej współpracy. Poznane rozwiązania i techniki prowadzonych działań w zakresie zwalczania przestępczości w obiegu elektronicznymi środkami płatniczymi, pozwolą na przekazanie zdobytej wiedzy innym policjantom, co wpłynie pozytywnie na ich kwalifikacje zawodowe, a jednocześnie pozwoli na wypracowanie własnych procedur postępowania w celu poprawy skuteczności działań Policji w walce z cyberprzestępczością.

Celem rozpowszechnienia, zdobytych podczas wymiany, nowych doświadczeń Wydział Doskonalenia Zawodowego KWP we Wrocławiu w kooperacji z wydziałami merytorycznymi, przygotuje program szkolenia w tym zakresie. Będzie on rozpowszechniany wśród policjantów garnizonu dolnośląskiego celem podniesienia wiedzy i świadomości w zakresie, coraz częściej stosowanej przez przestępców, drogi przestępczej z użyciem elektronicznych środków płatniczych.

Niniejszy projekt zapoczątkował roboczą współpracę policji dolnośląskiej i rumuńskiej w zakresie zwalczania przestępczości z użyciem elektronicznych środków płatniczych. Policjanci na bieżąco kontaktują się ze sobą i wymieniają informację, które w znaczącym stopniu ułatwiają prowadzenie prac operacyjnych, a tym samym zwiększają efektywność działań policyjnych i bezpieczeństwo użytkowników kart płatniczych.

5.1 Analiza porównawcza działalności przestępczej oraz metod jej rozwiązywania w Polsce i w Rumunii

W Polsce i Rumunii przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych, w szczególności kart bankowych, ma odmienne postaci i nasilenie.

Dla porównania, w Polsce w okresie 2007 r., najwięcej tego rodzaju przestępstw dotyczyło realizacji fałszywych kart bankowych w bankomatach, czyli wypłat gotówkowych dokonywanych przy pomocy fałszywych kart bankomatowych z BIN-ami (Bank Identification Number) angielskimi (kartami, które na paskach magnetycznych miały zakodowane dane – tzw. ścieżki – skopiowane wcześniej z kart banków wydawców z terenu Wielkiej Brytanii).

W 2008 roku tendencja ta uległa zmianie na rzecz skimmingu bankomatowego – kopiowania kart bankowych w bankomatach, a następnie wykorzystywania skopiowanych danych do produkcji fałszywych kart i ich realizacji w bankomatach za granicą (m. in. w Rumunii).

Na terenie Rumunii, z kolei większość przestępstw kartowych polega na dokonywaniu wypłat gotówkowych w bankomatach przy użyciu sfałszowanych kart z BIN-ami banków zagranicznych, jak również samej produkcji fałszywych kart bankowych, które realizowane są następnie na terenie Rumunii, jak i w innych krajach europejskich.

Metody pozyskiwania danych z kart bankowych, jak również fałszowania kart: płatniczych, bankomatowych, kredytowych, stosowane przez sprawców w Rumunii i w Polsce, jak zresztą na całym świecie są takie same. Jest to oczywiste z uwagi na międzynarodowy charakter tego rodzaju przestępczości. Dane z kart kopiowane są w drodze skimmingu (w szerokim znaczeniu kopiowania kart przy pomocy każdej metody), ale bardziej popularną metodą jest skimming bankomatowy (kopiowanie kart i jednoczesne sczytywanie numerów PIN w bankomatach). Zarówno w Polsce, jak i w Rumunii, największym zagrożeniem jest skimming bankomatowy.

Metody produkcji fałszywych kart są również podobne w obydwu krajach. Jednak ciekawostką jest, że policja w Rumunii odnotowuje mało już popularne w Polsce, czy też w krajach Europy Zachodniej, podrabianie kart stricte płatniczych, którymi sprawcy posługują się przede wszystkim w placówkach bankowych, ale również w bankomatach. Podrabianie kart polega na sfabrykowaniu plastiku znormalizowanego na wzór autentycznej karty bankowej, włącznie z szatą graficzną i

zabezpieczeniami lub bardzo profesjonalną imitacją zabezpieczeń stosowanych w kartach oryginalnych. Jedną z metod podrabiania kart, ujawnioną przez policję rumuńską w ramach likwidacji jednej z fabryczek fałszujących karty bankowe, jest metoda embossingu. Metoda ta polega na tłoczeniu znaków na karcie, na przykład: danych osobowych, numerów, dat ważności, jak też możliwości barwienia plastiku kart w kolorach matowych i metalicznych. Jest to jedna z bardziej profesjonalnych metod stosowanych przez sprawców fałszerstw kart na świecie.

Ściganie sprawców przestępstw z wykorzystaniem elektronicznych środków płatniczych przez polskie i rumuńskie organy ścigania jest w zasadzie podobne. Policje obu krajów współpracują w tym zakresie z policją innych państw, jak również z bankami, wydawcami kart, centrami autoryzacyjno-rozliczeniowymi, systemami kart (VISA, MasterCard itp.). To samo dotyczy współpracy z Interpolem i Europolem, których członkami jest zarówno Polska, jak i Rumuńska policja. Również oba kraje są pełnoprawnymi członkami AWF TERMINAL – elektronicznego analitycznego pliku roboczego działającego w strukturze Europolu, zadaniem którego jest gromadzenie, przetwarzanie i analizowanie wszelkich informacji i danych w zakresie przestępstw dotyczących kart bankowych z terenu całej Europy.

Regulacje prawne, istniejące w Polsce i w Rumunii, w odniesieniu do możliwości ścigania sprawców przestępstw z wykorzystaniem elektronicznych instrumentów płatniczych różnią się między sobą, jednak pozwalają skutecznie ścigać osoby podejrzane o dokonywanie tego rodzaju przestępstw. Odmienność wynika w szczególności z różnic w zakresie instytucji prawa karnego materialnego, jak i procesowego, jak też różniących się systemów prawnych. Na uwagę zasługuje fakt, że maksymalny wymiar kary dla sprawców fałszowania środków płatniczych, w tym również kart płatniczych, w Polsce jest znacznie wyższy niż w Rumunii. W Polsce taki czyn jest zbrodnią i jest zagrożony karą pozbawienia wolności do lat 25, w Rumunii kara za takie samo przestępstwo jest dużo niższa.

Reasumując, można stwierdzić, że pomimo braku zasadniczych różnic w obszarze przestępczości z wykorzystaniem elektronicznych instrumentów płatniczych, która występuje w Polsce i w Rumunii, jak również samej działalności policji obu krajów; metod rozpoznawania, ujawniania, ścigania i likwidowania tego rodzaju przestępczości, możliwość wymiany doświadczeń z policjantami rumuńskimi była nieoceniona. Zapoznanie się i omówienie poszczególnych odrębnych aspektów zagadnienia, jakim jest ściganie przestępstw z wykorzystaniem elektronicznych

środków płatniczych, miało duże znaczenie dla policjantów obydwu stron i wiele wniosło do ich praktyki i wiedzy.