„Stop fałszerstwom”

Wstępne rozpoznanie tematyki fałszerstwa

Zjawisko fałszowania dokumentów, banknotów, monet nie jest wbrew pozorom wynalazkiem rewolucji przemysłowej w XVIII wieku. Nie jest tym bardziej zwycięstwem myśli technicznej w wieku XX. Mimo iż obecne możliwości techniczne wyniosły ten przejaw działalności przestępczej na wyższy pułap, jego rodowód sięga już czasów starożytnych. Rozwojowi tego procederu od zawsze sprzyjał dynamiczny wzrost działań gospodarczych, finansowych oraz dostęp do wszelkiego rodzaju najnowocześniejszych technologii przy niskim poziomie zabezpieczeń. Szczególnie narażone były na to organy administracji państwowej lub sfera obrotu gospodarczego dokumentów. W dzisiejszych czasach gdy karty płatnicze stały się codziennością i coraz częściej dokonujemy za ich pomocą zakupów, jesteśmy w sposób znaczny narażeni na tego typu ryzyko. Czując się spokojniejsi kiedy nie mamy przy sobie gotówki, nie zdajemy sobie sprawy z pozorności naszego poczucia bezpieczeństwa. Wraz z powstaniem tej formy płatności pojawiła się nowa kategoria przestępstw - oszustwa dokonywane przy użyciu kart płatniczych zwane fraudami kartowymi. Dostrzegany obecnie dynamiczny rozwój tego typu naruszeń prawa i jest to oczywistą konsekwencją powszechności stosowania kart płatniczych.

Dokumenty standardowe natomiast tj. dowody, umowy, faktury itp., spełniają rolę narzędzia przestępstwa, za pomocą którego można popełnić kilkadziesiąt rodzajów różnych przestępstw. Szczególnie groźne, powodujące niejednokrotnie gigantyczne straty Skarbu Państwa, są przestępstwa gospodarcze.[1] Przykładami fałszerstwa, bardzo dotkliwymi dla zwykłych obywateli są różnego rodzaju oszustwa, przywłaszczenia mienia, wyłudzenia, kradzieże tożsamości itp.

Fałszowanie pieniędzy – zjawisko o bogatym rodowodzie

Fałszerstwa znaków pieniężnych towarzyszą człowiekowi od czasu pojawienia się w rozliczeniach finansowych monet, a następnie banknotów. Podrabianie lub obróbka pieniądza oraz częstotliwość ich fałszowania zależały od jego siły nabywczej w świecie. Znaczenie miał też sposób ich zabezpieczenia. Zawsze tam gdzie pojawiał się pieniądz wraz z rywalizacją na arenie międzynarodowej – istniało ryzyko, że jakieś państwo będzie chciało ingerować w interesy ekonomiczne sąsiadów.

Fałszowanie dokumentów nie jest zdobyczą czy dobrodziejstwem naszych czasów, lecz znane było już od dawna. Od momentu kiedy dokument, a ściślej mówiąc pismo bądź

waluta (w różnej formie) zaczęły pełnić formę pośrednika w wymianie myśli lub dóbr. Znane są fałszerstwa z czasów sumeryjskich i babilońskich, dokonane w imperium rzymskim i na innych terenach. Niewiele zachowało się jednak o nich bezpośrednich historycznych przekazów . Można być jednak pewnym, że po raz pierwszy pieniądz został sfałszowany w drugiej połowie VI w. p.n.e., kiedy to Polikrates - tyran z wyspy Samos - wynajął Spartan jako wojsko zaciężne. Po wygranej przez nich kampanii zapłacił im z góry ustaloną sumę złotymi monetami, tyle że sfałszowanymi. Pieniądze te były podrobione techniką platerowania - krążek z miedzi lub cyny otaczano cienką blaszką ze złota lub srebra i taką „metalową kanapkę" bito stemplem. W końcówce wieku VI p.n.e. wyrabianie fałszywych monet było dużym problemem gospodarczym i stanowiło nie lada wyzwanie dla ówczesnych prawodawców. Na przykład w słynnych prawach Solona, przewidziano za tego typu działalność karę śmierci. Przez wiele wieków przestępcy pokrywali rdzeń, wykonany z nieszlachetnego metalu, cienką warstwą srebrnej blachy. Tak spreparowany pieniądz wprowadzano do obiegu jako autentyczną monetę. Potrzeba kontroli jakości monet oraz wyeliminowania tych „psutych" z obiegu zmusiła Greków do wynalezienia prymitywnej jak na owe czasy, choć skutecznej metody weryfikacji autentyczności tych podejrzanych, poprzez nacięcie obrzeża monety ostrym narzędziem. Nie tak rzadkie musiały być również fałszerstwa w średniowiecznej Europie, skoro zasady badania autentyczności dokumentów formułowali papieże: Innocenty III, Aleksander II, Grzegorz IX, Innocenty IV i inni.

Już w starożytności pojawiły się bardziej lub mniej wyszukane lecz raczej prymitywne w swej formie, fałszerstwa zapisów. Bywały to często fałszerstwa dokonywane niejako w majestacie prawa, przez władców lub osoby wysoko postawione w hierarchii społecznej. Nawet tak znamienity prawodawca, jakim był cesarz Justynian, nie ustrzegł się przed łatwym do wykrycia fałszerstwem o charakterze publiczno-prawnym. Komisji, opracowującej pomniki prawodawstwa rzymskiego, zalecił mianowicie „*dokonanie wszelkich potrzebnych zmian tekstu*". Podkreślił również, aby zmian tych „*nie zaznaczono wyraźnie, lecz włączono je tak, ażeby wyglądały na tekst pierwotny*".[2]

Przykłady fałszerstw w Polsce

Pierwsza sfałszowana polska moneta to denar krzyżowy z IX wieku, wykonany z miedzianej płytki pokrytej cienką srebrną blaszką. W 1380 roku głośno było o warsztacie fałszerskim w zamku w Szaflarach na Podhalu, gdzie srebrne, złote i miedziane falsyfikaty wybijane były przez pewnego Żyda. Fałszerze działający w średniowiecznej Polsce, poza przerabianiem zapisów i fałszowaniem monet, znaleźli dla siebie wspaniałe warunki

w instytucji zwanej transumptem. Było to sporządzanie odpisu, który po potwierdzeniu miał moc prawną dokumentu. Oryginał dokumentu mógł więc w tych warunkach zaginąć co bardzo często miało miejsce. Dość powszechnie korzystano z instytucji transumptu, przerabiając „zapiski". Były to różnego rodzaju dokumenty klasztorne lub kościelne. Charakteryzowały się tym, że były sporządzane w osobie trzeciej i dotyczyły nabytków klasztornych, rzeczywistych lub domniemanych. W momencie uznania za stare, dokumenty przeredagowywano i zaopatrywano w znamiona autentyczności.[3]

Powyższe działania przypominają dzisiejsze „poświadczenia za zgodność z oryginałem" i dokonywane są bardzo często w odniesieniu do dokumentów nieautentycznych, które jako oryginały są przedstawiane nieświadomym tego faktu notariuszom lub urzędnikom administracji publicznej do potwierdzenia. Po uzyskaniu takiej zgodności dokument sfałszowany może rozpocząć samodzielny byt dokumentu autentycznego, a w rzeczywistości takiego, którego nieautentyczność została zalegalizowana. W obecnym polskim prawodawstwie działanie to zagrożone jest sankcją karną zawartą w rozdziale XXXIV Kodeksu Karnego RP dotyczącego przestępstw przeciwko wiarygodności dokumentów. Zawarty w nim Art. 272. stanowi: Kto wyłudza poświadczenie nieprawdy przez podstępne wprowadzenie w błąd funkcjonariusza publicznego lub innej osoby upoważnionej do wystawienia dokumentu, podlega karze pozbawienia wolności do lat 3. W dalszej części, Art. 273. stanowi: Kto używa dokumentu określonego w art. 271 lub 272, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Artykuł nr 271 poprzedzający w KK dwa wcześniej wymienione, w trzech zawartych w nim paragrafach mówi o odpowiedzialności karnej funkcjonariuszy publicznych wystawiających nieprawdziwe dokumenty i/lub czerpiących z tej działalności korzyści majątkowe lub osobiste. [4]

Jednym z najbardziej znanych polskich przypadków działalności fałszerskiej jest okres fałszowania monet Królestwa Polskiego w latach 1740–1786. Za panowania Sasów Polska poniosła dotkliwe straty gospodarcze wskutek podrabiania polskich monet przez króla pruskiego Fryderyka II. W mennicach na terenie Prus i Niemiec produkowano srebrne i złote monety polskie. Proceder odbywał się techniką fałszywych stempli z wygrawerowanym popiersiem króla Augusta III. Najbardziej precyzyjne podróbki robione były za pomocą w/w stempli wykonanych na wzór oryginalnych monet. Rysunek monety rzeźbiono lub odlewano w miękkim metalu, by następnie hartować ją do otrzymania pożądanej jakości.
Tego typu monety miały gorszy dźwięk i mniej precyzyjny rysunek. W monetach tych także znajdowała się spora domieszka miedzi, ale miały patynę koloru srebra i wyglądały dość wiarygodnie. Proces „wypierania" w ten sposób uzyskanych pieniędzy polegał na

przywożeniu falsyfikatów do Polski i wymianie ich na dobre polskie monety z czystego srebra. W niektórych przypadkach by uniknąć zbyt szybkiego wykrycia po prostu kupowano u rzemieślników srebrne i złote wyroby. Nie trzeba wspominać, że w wyniku tego procederu Polska utraciła setki milionów złotych i poniosła straty trudne do odrobienia.
Na odrębną uwagę zasługuje rozdział w historii fałszerstw dotyczący banknotów.
Wśród mnogości falsyfikatów pieniądza papierowego wyróżnia się następujące kategorie:

podrobione (fałszywe – wykonane od podstaw przez fałszerza),

przerobione (sfałszowane – na których podwyższono nominał oraz zmieniono pozostałe elementy graficzne),

preparowane (powstałe w wyniku cięcia i sklejania ze sobą odcinków banknotów o zmniejszonym rozmiarze, pierwotnie do siebie nie należących).

Różnice jakie pozwalają odróżnić banknoty fałszywe od autentycznych to przede wszystkim: gatunek papieru, grafika oraz zabezpieczenie. Rysunek falsyfikatu oraz jego poszczególne elementy, wykonane w oryginale techniką stalorytniczą powodowały że banknot był nieostry i bez wyrazu.[5]

Największą aferą fałszerską w czasach II Rzeczpospolitej było wykrycie kolporterów fałszywych banknotów o nominale 20 zł w 1933 roku. Okazali się nimi z pozoru niewinni kasjerzy z Dworca Głównego w Warszawie, którzy wydawali falsyfikaty jako resztę za zakupiony bilet. W czasie II wojny światowej Polacy masowo fałszowali hitlerowskie banknoty okupacyjne tzw. młynarki, co traktowano jedynie jako mały sabotaż. Niemcy jednak, stanowczo wyciągnęli wnioski z sukcesów w fałszowaniu młynarek, dlatego w specjalnym bloku w obozie koncentracyjnym w Sachsenhausen zorganizowali drukarnię fałszywych funtów brytyjskich i dolarów. Przedsięwzięcie o kryptonimie „Operacja Bernhard" miało na celu destabilizację brytyjskiego systemu monetarnego w ramach prowadzonej na równi z działaniami wojskowymi, wojny ekonomicznej. [6] Po wymianie pieniędzy w Polsce w 1950 roku, pierwsze falsyfikaty pojawiły się w obiegu dopiero w 1955 roku. Z czasem umiejętności i możliwości polskich fałszerzy rosły. W latach osiemdziesiątych fałszowano w Polsce więcej obcych walut a w szczególności dolarów i marek zachodnioniemieckich. Podrabianie polskich banknotów w tamtym czasie zeszło na drugi plan. Początek lat 90. przyniósł zmiany w kodeksie karnym. Przestał obowiązywać artykuł, który mówił o zorganizowanej działalności godzącej w interes państwa oraz

drugi - o niegospodarności w zarządzaniu mieniem społecznym. To stworzyło próżnię, w którą natychmiast weszły gangi i zorganizowane grupy przestępcze, również o charakterze międzynarodowym, zalewając Polskę sporą ilością podrobionych pieniędzy. Polskie banknoty wyemitowane 1 stycznia 1995 roku otrzymały najlepsze jak na tamte czasy zabezpieczenia przed fałszerstwem**.** W ślad za nami poszła Szwajcaria, emitując w 1995 roku lepiej chronione przed podrabianiem franki.

Euro – wspólna waluta i wspólne ryzyko zjednoczonej Europy

Banknoty euro weszły do obiegu w 2002 roku. Nie mają jednak zbyt dobrego zabezpieczenia, czego dowodem są liczne doniesienia w mediach o kolejnych przypadkach fałszerstw tych banknotów Od początku 2002 r. w 12 krajach Europy weszło do obiegu 14 mld nowych banknotów euro. Wprowadzenie nowej waluty wiązało się z podjęciem przez władze krajów europejskich różnorodnych środków mających na celu przeciwdziałanie próbom fałszerstw. W procesie projektowania i produkcji banknotów euro, twórcy wykorzystali najbardziej zaawansowane technologie zabezpieczeń. Podobnie jak w przypadku przestępstw komputerowych, wraz z rozwojem technik hakerskich, administratorzy stają niemal na głowie by być krok przed swoimi oponentami, tak samo w przypadku fałszerstw, nie poprzestano na jednej, sprawdzonej technologii. Jest ona cały czas rozwijana i w najbliższej przyszłości możemy spodziewać się wielu zmian w zabezpieczeniach. Europol (policja europejska), przy współpracy z rządami wszystkich krajów Unii Europejskiej, podejmuje działania mające zapobiec fałszerstwom dokonywanym przez zorganizowane grupy przestępcze. Czynnikiem wspierającym te działania jest kara ośmiu lat więzienia, która grozi za fałszowanie nowej waluty.

Niezależnie od podejmowanych działań, wprowadzenie nowych banknotów na rynek stanowi znakomitą okazję dla fałszerzy. Szczególnie w początkowym okresie funkcjonowania euro należało liczyć się z tym, że fałszerze będą podejmować próby reprodukowania banknotów przy wykorzystaniu zaawansowanych urządzeń drukująco – kopiujących. Warto przytoczyć tutaj wypowiedź Jeana-Noëla Machona, prezesa oddziału firmy Xerox na Europę, firmy która jako jedna z pierwszych wyszła naprzeciw potrzebom zapobiegania fałszerstwom banknotów:

„Technologia druku cyfrowego jest obecnie tak zaawansowana, że można stworzyć dokładną reprodukcję nawet najbardziej skomplikowanych wzorów i kombinacji kolorów”.

W ciągu kilku ostatnich lat bardzo wiele firm-producentów drukarek, kopiarek, skanerów przeznaczyło znaczne nakłady na technologię zapobiegania fałszerstwom. Ich urządzenia zostały wyposażone w systemy uniemożliwiające kopiowanie rozpoznanego banknotu. W przypadku, gdy ktoś próbuje manipulować przy systemach zabezpieczających, uruchamia się blokada zatrzymująca pracę urządzenia. Innym sposobem przeciwdziałania fałszerstwom jest system znakowania, polegający na umieszczaniu tajnego kodu na każdym arkuszu wydrukowanym na drukarce. Odczytanie kodu pozwala instytucjom wymiaru sprawiedliwości na szybkie zidentyfikowanie urządzenia, na którym została wykonana kopia. W przypadku przedsiębiorstw i instytucji korzystających z kolorowych kopiarek podłączonych do sieci możliwe będzie nawet ustalenie tożsamości osoby, która sporządziła kopię. Jak widać kroki powzięte w celu walki z fałszerstwem i innymi zagrożeniami płynącymi bezpośrednio od niego, są na znacznym stopniu zaawansowania technicznego. Obecny rozwój techniki oraz sprawność monitorowania Internetu przez odpowiednie służby sprawiają, że potencjalni fałszerze nie mogą czuć się już tak bezkarni jak choćby 10 czy 15 lat temu. Wszyscy producenci kolorowych kopiarek i drukarek zdają sobie sprawę, że barwna technologia przetwarzania obrazu może służyć do podrabiania pieniędzy, niosąc ze sobą zagrożenie dla światowego systemu walutowego. Wyposażanie urządzeń drukujących w zabezpieczenia jest jedną z form przeciwdziałania temu procesowi.

Kilka lat temu słynna była w Polsce sprawa dokonania kradzieży, przez jedną ze zorganizowanych grup przestępczych pięciu ton papieru do produkcji banknotów. Papier wytworzono w Niemczech, a przeznaczony był dla Rosji oraz jej wewnętrznego zapotrzebowania. Transport od przekroczenia granicy niemieckiej, kontrolowany był przez UOP (Urząd Ochrony Państwa – obecnie Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu). Zawartość transportu została zrabowana podczas brawurowej akcji bandytów. Zanim oficerowie UOP-u zorientowali się co się tak naprawdę stało, ładunek zniknął. Po jakimś czasie 3,7 tony tego papieru zostało oddane agentom UOP, dzięki negocjacjom prowadzonym przez ówczesnego szefa CBŚ (Centralne Biuro Śledcze) Adama Rapackiego, negocjującego warunki z przedstawicielami grupy. 1,3 tony zostało natomiast wykorzystane, jak się później okazało do wydrukowania rubli, które nawet rosyjscy specjaliści po wstępnych analizach uznali za autentyczne. Świadczy to o łatwym dostępie bandytów do zaawansowanych technologii druku, w tym także cyfrowego. Wydawałoby się, że ilość papieru nie była zbyt duża jak na warunki tak wielkiego państwa jakim była i jest Federacja Rosyjska. Prawda jest jednak zupełnie inna. Z takiej ilości papieru można było w tamtym czasie wyprodukować i wprowadzić do obrotu tak dużą ilość banknotów, że przy chwiejącej

się gospodarce po neoliberalnych reformach Jelcyna, mogło w bardzo realistyczny sposób zagrozić systemowi ekonomicznemu Rosji.

Europejski Bank Centralny twierdzi, że przy produkcji banknotów euro stosuje się wyrafinowane techniki drukarskie. Mimo to zalecane jest częste sprawdzanie kilku zabezpieczeń naraz. Zajmuje to zaledwie kilka sekund ale może oszczędzić wielu nieprzyjemności. Banknoty mają też szereg łatwo rozpoznawalnych zabezpieczeń, które umożliwiają wykrywanie falsyfikatów nawet bez specjalistycznego sprzętu i utrudniają fałszerstwa. Do wspomnianych środków prewencyjnych zaliczyć należy:

wyposażenie banknotów euro w zabezpieczenia, umożliwiające rozpoznanie prawdziwych banknotów na pierwszy rzut oka,
wypukły nadruk uzyskiwany w specjalnym procesie drukarskim, łatwo wyczuwalny opuszkami palców,
pasek zabezpieczający, znak wodny oraz cyfry uzupełniające się pod światło (wszystkie te trzy elementy są widoczne po obu stronach autentycznych banknotów, w razie wątpliwości warto spojrzeć na banknot pod światło),
motyw graficzny na hologramie, zmieniający się w zależności od kąta patrzenia (na odwrotnej stronie można zobaczyć złocisty pas przy nominałach 5 €, 10 € i 20 € lub nominał zmieniający kolor jak w przypadku banknotów 50 €, 100 €, 200 € i 500 €),

Dodatkowe techniki ochrony przed fałszywymi pieniędzmi

W celu wzmocnienia ochrony przed przyjęciem fałszywych banknotów warto zainwestować w profesjonalna lampę kasjerską, która być może nie zawsze da pewności w 100% ale na pewno pomoże w dużym stopniu wykryć fałszywe pieniądze lub próbę wprowadzenia ich do sprzedaży. Jeżeli ktoś prowadzi biznes, w którym obrót „żywym" pieniądzem jest systematyczny i szybki, powinien rozważyć zakup takiego urządzenia. Niewielkich rozmiarów, dyskretna lampa doskonale oświetla banknoty, pozwalając dostrzec nawet najtrudniejsze do wykrycia zabezpieczenia, takie jak efekt kątowy czy zabezpieczenia optyczne. Obecnie jest na polskim rynku kilka takich lamp kasjerskich, które wykorzystując refleksyjne białe światło do rozpoznawania zabezpieczeń banknotów nie wymagając przy tym przerywania ich liczenia, ponieważ pieniądze nie są do nich wkładane, a ich autentyczność weryfikowana jest tylko w świetle urządzenia. Znacznie przyspiesza to pracę kasjerów oraz zmniejsza obciążenie psychiczne. Dodatkowym elementem chroniącym przed fałszywkami są szkolenia z zakresu rozpoznawania falsyfikatów oraz

zabezpieczeń stosowanych obecnie we wszystkich walutach świata, organizowane przez wiele firm. W trakcie szkolenia, uczestnicy poznają przede wszystkim cechy banknotów oryginalnych (jak choćby wspomniane wyżej cechy waluty euro) i ich zabezpieczenia. Uczą się rozpoznawać unikalne cechy prawdziwych banknotów i monet, także zapoznają się z najnowszymi światowymi trendami w fałszowaniu pieniędzy. Dla przykładu - szkolenie dla pracowników obsługi banków oraz kantorów opiera się w znacznej większości na :

1.Zabezpieczeniu identyfikacji dokumentów

zabezpieczenia w druku
zabezpieczenia w rysunku
zabezpieczenia optyczne
identyfikacja dokumentów tożsamości: dowód osobisty, paszport obywatelski i obywatelski biometryczny
identyfikacja dokumentów stwierdzających uprawnienia do kierowania pojazdem: prawo jazdy
rozpoznawanie zabezpieczeń dokumentów
weryfikacja przedstawianych dokumentów

oraz

2.Sposobach i metodach fałszowania dokumentów publicznych i prywatnych

tworzenie dokumentów od podstaw: dla konkretnych potrzeb oraz ich podrabianie
zmiana oryginalnych dokumentów: w zależności od potrzeb i przerabianie
kradzież tożsamości: podrabianie wszelkiego rodzaju dokumentów potwierdzających tożsamość

Złożoność zagadnień, wymienionych powyżej treści szkoleń świadczy o głębi tego zjawiska i o rzeczywistym zapotrzebowaniu na tego typu szkolenia.[7] Pozwala to także uzmysłowić sobie wielość płaszczyzn na jakich funkcjonują osoby zajmujące się fałszowaniem dokumentów. Oczywiście zwyczajnemu obywatelowi takie szkolenie nie jest do niczego potrzebne. Warto jednak zdać sobie sprawę, że należy być czujnym w takim przypadku gdy chodzi o nasze pieniądze i o nasze dobro. Poznanie kilku dystynktywnych cech waluty jaką na co dzień się posługujemy może okazać się nieocenione i pozwoli uniknąć przykrych sytuacji.[8]

Fałszowanie dokumentów tożsamości

Obecnie fałszerstwa dotyczą niemalże wszystkich rodzajów dokumentów np. biletów (komunikacji miejskiej, biletów wstępu), przez dokumenty cywilnoprawne (świadectwa, testamenty, umowy, zobowiązania), dokumenty samochodowe, dokumenty związane z obrotem towarowym i działalnością gospodarczą (np. dokumenty celne, faktury, znaki towarowe, znaki akcyzy), oświadczenia skarbowe, rachunki, dokumenty firmowe, legalizujące działalność gospodarczą, fałszerstwa związane z bankowością (umowy kredytowe, karty płatnicze, czeki, polecenia przelewu, poręczenia, weksle itp.)

Problem ten pojawia się, poczynając od fałszerstw najbardziej trywialnych wspomnianych na początku tego podrozdziału, lecz co zrobić gdy złodzieje sięgają po naszą tożsamość, próbując za jej pomocą osiągać korzyści. Należy pamiętać, że banki nie posiadają wglądu do policyjnej bazy i podczas załatwiania formalności nie mają fizycznej możliwości sprawdzenia czy dany dokument nie figuruje jako skradziony.

Codziennie kilku oszustów w kraju próbuje zaciągnąć kredyt na skradziony lub sfałszowany dowód osobisty. Ze statystyk wynika, że w Polsce średnio kilka razy dziennie ktoś próbuje wziąć kredyt na nie swój dowód. Dlatego bardzo ważne jest zgłoszenie kradzieży do bazy prowadzonej przez Związek Banków Polskich. Aby uchronić się przed kradzieżą dokumentu, której najczęstszym następstwem jest bezprawne użycie skradzionego identyfikatora lub jego odpowiednia obróbka, przez osoby trzecie, należy pamiętać o nie eksponowaniu swoich dokumentów oraz zwrócenie uwagi na obcych kręcących się w pobliżu. Sposoby fałszerstw tych dokumentów i ich zakres rozwijały się. Równocześnie rozwijały się też środki mające zapobiec powstawaniu podrobionych dokumentów, między innymi metody technicznego ich badania. Rozmiar tych badań zależał od stopnia społecznego i prawnego rozwoju konkretnego społeczeństwa oraz od warunków technicznych.

Oszustwa związane z weryfikacją tożsamości na podstawie dowodu elektronicznego

Przekonanie o prawdziwości dowodu elektronicznego nie może opierać się na zapewnieniach urzędu państwowego, że dowody są dobrze zabezpieczone. Obywatel powinien mieć możliwość samodzielnego sprawdzenia czy dowód elektroniczny jest prawdziwy tak jak w przypadku dowodu książeczkowego używane wcześniej.

Dowód elektroniczny staje się coraz bardziej popularną formą dokumentu tożsamości w krajach wysoko i średnio rozwiniętych gdzie posiadanie plastikowej karty z danymi jest już codziennością. Ten rodzaj dokumentu charakteryzuje się plastikową kartą z wbudowanym

komponentem elektronicznym. Tożsamość obywatela w elektronicznym dowodzie jest określana za pomocą trzech rodzajów atrybutów:

identyfikatory urzędowe (nadane lub zatwierdzone przez urzędy): imię, nazwisko,

data urodzenia, miejsce urodzenia, imiona rodziców, adres zameldowania, PESEL

cechy charakterystyczne wyglądu: obraz twarzy, płeć, wiek, wzrost, kolor oczu

cechy biometryczne(w postaci cyfrowej): geometria twarzy, linie papilarne, etc.

Identyfikatory urzędowe mają charakter umowny i większość z nich może być zmieniona. Sprawdzenie tożsamości na podstawie dowodu polega na porównaniu cech charakterystycznych wyglądu na dowodzie z rzeczywistym wyglądem osoby podającej się za jego właściciela. Jeżeli cechy charakterystyczne osoby na dowodzie pokrywają się z jej wyglądem i dowód nie jest podrobiony, to uznać należy prawdziwość identyfikatorów urzędowych. Jeśli dowód zawiera wzorzec cechy biometrycznej to można dodatkowo sprawdzić czy próbka biometryczna zeskanowana z osoby podającej się za właściciela dowodu jest zgodna z tym wzorcem. Zwiększanie szczegółowości cech charakterystycznych wyglądu przeciwdziała oszustwom. Im większa czytelność cech charakterystycznych wyglądu na dowodzie tym trudniej oszukać sprawdzającego. Silnym mechanizmem zabezpieczającym przed oszustwem jest zatem weryfikacja cech biometrycznych. Do dokonania oszustwa mogą być użyte różnego rodzaju fałszywe dowody:

dowód oryginalny z przerobionymi danymi

dowód oryginalny z nieprzerobionymi danymi, które są fałszywe (taki dowód można zdobyć przez wykorzystanie słabości procesu wydawania dowodów)

dowód podrobiony (na podrobionym blankiecie)

Dowód elektroniczny jest personalizowany wizualnie i elektronicznie w procesie jego wydawania. Personalizacja wizualna może być wykonana tylko raz jeśli dowód ma być zabezpieczony przed przerabianiem nadruku. Dane elektroniczne można zapisać jednorazowo lub wielokrotnie w zależności od tego czy nośnik pamięci komponentu elektronicznego umożliwia kasowanie danych czy nie. Konstrukcja systemu zabezpieczeń dowodu elektronicznego musi bazować na kompromisie między prostotą a skutecznością. Współczesne technologie umożliwiają wbudowanie w komponent elektroniczny ogromnej liczby funkcji użytkowych i serwisowych. Ilości tych funkcji musi być ograniczona do

niezbędnego minimum, tak aby zminimalizować ryzyko pojawienia się nieprzewidzianych zastosowań dla dowodu i danych w nim zgromadzonych. Mogłyby być one groźne dla jego właściciela lub uderzałyby w jego interesy. Istotną rzeczą przy weryfikacji prawdziwości takich dokumentów często pomijana w pracach jest tzw. czynnik ludzki. Dotyczy to osoby weryfikującej podejrzane dokumenty. Wypracowanie nawyku kontroli dokumentów jakie są przedstawiane pozwala zminimalizować ryzyko bycia oszukanym. Biorąc dokument do rąk należy przede wszystkim zwrócić uwagę na cechy charakterystyczne wyglądu w dowodzie z rzeczywistym wyglądem osoby podającej się za jego właściciela.
Jeśli cechy charakterystyczne osoby na dowodzie pokrywają się z jej wyglądem i dowód nie jest podrobiony w inny sposób, to uznać należy taki dokument za prawdziwy identyfikator urzędowy. [9]

Podpis elektroniczny – niepewna przyszłość nowej technologii

Ustawa o podpisie elektronicznym z dnia 18 września 2001 r. wprowadziła Polskę do nielicznego grona krajów, w których istnieje możliwość przekazania za pośrednictwem poczty elektronicznej dokumentu, mogącego mieć prawne znaczenie takie samo, jak dokument podpisany osobiście przez autora.

Składanie podpisu odręcznego, stosowane dotychczas na wszelkiego rodzaju dokumentach, w celu nadania im cech prawnego środka wyrażenia woli osoby podpisującej, w wielu przypadkach wymaga osobistego wykonania podpisu przez zainteresowanego, w obecności urzędnika przyjmującego taki dokument. Podpis elektroniczny został stworzony dla zwiększenia podstawowego atutu poczty elektronicznej, jakim jest szybkość przekazu informacji. Nie trzeba podkreślać, że forma standardowego podpisu stanowi zaprzeczenie idei poczty elektronicznej jako błyskawicznego sposobu przekazywania danych.
Podpis elektroniczny jest ściśle związany przede wszystkim z działalnością banków, firm i instytucji, które dokonują wypłat i przelewów pieniężnych przy wykorzystaniu poczty e-mail. Podpis cyfrowy jest to kryptograficzne przekształcenie jednostki danych umożliwiające odbiorcy sprawdzenie pochodzenia i integralności w/w jednostki oraz ochronę odbiorcy informacji przed sfałszowaniem jej przez nadawcę. Idea funkcjonowania podpisu elektronicznego może działać w momencie gdy jest zapewniona podstawowa współpraca nadawcy i odbiorcy informacji. Odbiorca musi mieć absolutną pewność oraz pełne zaufanie, że osoba składająca podpis elektroniczny jest faktycznie tą, która podaje się za autora informacji czy decyzji. Istotną rzeczą jest zapewnienie całkowitej integracji podpisanego dokumentu (niemożność wprowadzenia zmian przez inne osoby), zabezpieczenie

niezaprzeczalności podpisu (uniemożliwienie stwierdzenia, że dokument został podpisany przez inną niż upoważniony osobę). W tym celu stosuje się przemyślne techniki kryptograficzne obejmujące wszelkie zagadnienia związane z ukrywaniem informacji. Technologia stosowana w przypadku podpisu elektronicznego oparta jest na pomyśle z lat 70, zwanym szyfrowaniem asymetrycznym. W metodzie tej klucz szyfrującego i deszyfrującego są takie same. Nadawca i odbiorca posługują się tym samym kluczem, który musi być utrzymywany w tajemnicy. Podany wyżej sposób szyfrowania opiera się na przekształceniach matematycznych tekstu (informacji), przy założeniu, że algorytm przekształcenia jest znany zainteresowanym. Skuteczność tej metody zależy od stopnia utajnienia informacji w parametrze zwanym kluczem. Im bardziej skomplikowany i utajony jest klucz, tym większe bezpieczeństwo, że osobom nieupoważnionym nie uda się go złamać.

Podstawowym problemem związanym z szerokim zastosowaniem podpisu elektronicznego jest konieczność stworzenia odpowiedniej infrastruktury opartej na oprogramowaniu, technikach szyfrowania, certyfikatach. Budowa odpowiedniego środowiska technicznego jest bardzo kosztowna. Koszt takiej budowy wacha się od kilku do kilkudziesięciu mln. USD, co drastycznie wydłuża proces wdrożenia takiego podpisu do użytku publicznego. Kolejną kwestią jest wykorzystanie podpisu w różnych sferach życia. Aby zapewnić jego skuteczne działanie należy dostosować szereg przepisów prawnych, zarówno z dziedziny prawa cywilnego, handlowego jak i karnego. Aktualne przepisy i związane z nimi tryby postępowania, nie uwzględniają całkowicie funkcjonowania takiej formy wyrażania woli, jaką jest podpis cyfrowy. Najważniejszą kwestią, jest status bezpieczeństwa całej procedury podpisu. Brak jest wieloletnich gwarancji dotyczących aktualnie stosowanych środków kryptograficznych. Fakt, że firmy zajmujące się tworzeniem oprogramowania szyfrującego nie dają wieloletnich gwarancji użytkownikowi swojego oprogramowania, podyktowane jest szybkim rozwojem technik hakerskich oraz metod łamania kluczy. Trudno jest przewidzieć kierunki rozwoju informatyzacji życia ludzkiego. Należy zwrócić uwagę na fakt, że podpis odręczny jednoznacznie identyfikowany jest z autorem za pomocą ekspertyz grafologicznych. W przypadku ustalenia związku nadawcy z dokumentem elektronicznym, ustalenia prowadzą jedynie do adresu IP komputera. Co zrobić zatem, w przypadku gdy z jednego komputera korzysta kilka osób lub gdy kontrola nad komputerem została utracona w skutek działania np. hakera? Obecny poziom zabezpieczeń teleinformatycznych pozostawia wiele do życzenia. Wątpliwości z tym związane spowodowały, że podpis elektroniczny funkcjonuje w wielu państwach, jak choćby w USA, Austrii w formie testowej i nie został wprowadzony do powszechnego użytku.

Z analiz ekspertów wynika, że musi jeszcze upłynąć kilka lat, nim przydatność i niezawodność tej technologii zostaną potwierdzone. [10]

Organy ochrony przed fałszerstwem oraz oszustwem

Rozpoznanie nowych zjawisk przestępczych, dokonywanych przy wykorzystaniu Hi-Tech oraz opracowanie metod działania spoczywa w rękach odpowiednich organów państwowych. Zwalczanie naruszeń praw autorskich i pokrewnych, praw do znaków towarowych, patentów i wzorów użytkowych leży w kompetencjach odpowiednich pionów wchodzących w skład Policji (Wydziały do Walki z Przestępczością Gospodarczą).
W Polsce za ujawnianie i zwalczanie piractwa odpowiedzialny jest Zespół do Zwalczania Przestępczości Intelektualnej, Komputerowej i Kartowej Centralnego Biura Śledczego KGP, będący częścią wydziału VI CBŚ Komendy Głównej Policji. Do jego głównych zadań należą:

Ochrona praw własności intelektualnej (praw autorskich, praw własności przemysłowej)
Ujawnianie i zwalczanie piractwa programownego, filmów, muzyki
Ustalanie oszustów działających na aukcjach w witrynach internetowych
Ustalanie sprawców ataków na systemy informatyczne (w tym przestępstwa z kradzieżą sygnału telewizyjnego)

W procesie monitorowania sieci Internet Policja stara się uzyskiwać informacje na temat działalności przestępczej, która wspierana jest przez najnowsze technologie.
W dziedzinie zwalczania przestępstw przeciwko elektronicznym systemom płatniczym (kartom płatniczym itp.), Policja współpracuje z bankowymi i nie bankowymi agencjami rozliczeniowymi (PolCard, BZWBK, CitiHandlowy, E-Card, American Express i inne) w zakresie koordynacji działań swoich jednostek terenowych w zwalczaniu fraudów kartowych. Wymieniając informacje z wyspecjalizowanymi policjami i instytucjami w innych państwach, w tym z centralą Europolu w Hadze, w zakresie przestępczości związanej z elektronicznymi instrumentami płatniczymi, uzyskuje dostęp do wielu specjalistycznych analiz oraz usprawnia system walki z tego typu procederami, unowocześniając metody działania. Poza własnymi ustaleniami w w/w zakresie specjalne zespoły wykonują wiele czynności usługowych w postaci ustaleń dla jednostek terenowych policji, których wyposażenie lub brak specjalistycznej wiedzy uniemożliwia realizację tych zadań. Z drugiej jednak strony, rosnąca w Polsce liczba przestępstw, popełnianych z użyciem wysoce

specjalistycznej technologii komputerowej, sugeruje że ilość zespołów specjalizujących się w ich wykrywaniu powinna zostać rozszerzona do jednostek terytorialnych(komendy wojewódzkie, powiatowe). Aktualne usytuowanie zespołów w strukturze CBŚ KGP, wydaje się być w miarę optymalne z uwagi na możliwości wykonawcze zadań i koordynacji pracy Policji.

Przestępstwa związane z wykorzystaniem kart płatniczych

Karty bankowe stanowią nieodłączny element naszej rzeczywistości, a ich posiadanie stało się niemal koniecznością. Pierwsze karty płatnicze pojawiły się w latach dwudziestych. W swojej krótkiej, lecz burzliwej historii przeszły wiele transformacji.

Rozwój i bezpieczeństwo to największe wyzwanie dla wydawców plastikowego pieniądza. Jego realizacja jest zatem niezbędna do utrzymania wzrostowej tendencji wśród użytkowników. Warto mieć na uwadze, 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 bankach jak i w policji, monitorujących wszystkie transakcje dokonywane kartami płatniczymi. Jednostki te podejmują szereg działań prewencyjnych w celu zminimalizowania ryzyka.

Fraudy kartowe stanowią w chwili obecnej największy odsetek nielegalnych transakcji dokonywanych za pomocą kart. Korzystanie z karty płatniczej wydaje się być dużo bardziej bezpieczne niż noszenie przy sobie gotówki. W razie kradzieży do momentu zastrzeżenia utraconej karty, prawo zapewnia nam ochronę od skutków nieuprawnionych transakcji od 150 euro wzwyż. Oznacza to, że konsekwencje materialne powyżej tej kwoty od chwili zastrzeżenia plastiku pokrywa bank. Pomimo, że poczucie bezpieczeństwa wypływające ze świadomości nie posiadania przy sobie sporej gotówki jest iluzoryczne, w ostatnim czasie liczba osób występujących o wydanie kart płatniczych, kredytowych diametralnie rośnie. We wstępie pracy wspomniane zostały statystyki wzrostu przestępczości mającej za swój przedmiot właśnie wszelkiego rodzaju karty. Przestępstwa ze zgubionymi lub skradzionymi kartami charakteryzują się tym, że sprawcy po wejściu w posiadanie takiej karty, nie zmieniając danych na karcie - podszywają się pod autentycznego posiadacza, fałszując podpis na rachunkach obciążeniowych, przy czym wykorzystują do tego wzór podpisu na karcie. Transakcje z bankomatów są możliwe tylko w przypadku, gdy PIN kod znajdował się razem z

kartą (np. był zapisany na karcie lub znajdował się w portfelu razem z kartą i innymi dokumentami). Nigdy, pod żadnym pozorem nie należy więc przechować zapisanego numeru w komórce lub w portfelu pod hasłem "PIN" ani podawać go innym osobom, o pożyczaniu swojej karty komukolwiek nie wspominając. Jest ona przypisana do jednego, określonego użytkownika i udostępnienie jej osobie trzeciej oznacza, że w przypadku kradzieży, ubezpieczenie kosztów nieuprawnionych transakcji nie będzie obowiązywać. Zwykle koszt takiego ubezpieczenia nie przekracza kilku złotych miesięcznie i chroni użytkownika nie tylko przed rabunkiem gotówki wypłaconej z bankomatu oraz kradzieżą samej karty i dokumentów, ale także zapewnia ubezpieczenie przedmiotów zakupionych kartą.

Fałszowanie kart jest procederem dość szeroko rozpowszechnionym zarówno za granicą, jak i w naszym kraju. W procesie użytkowania kart pojawiło się wiele innych przykładów przestępstw zajmujących dalsze miejsca wśród zagrożeń związanych z obrotem kartami płatniczymi. Najczęstsze przypadki to:

Podrobienie karty - karty są wykonywane przez fałszerza w oparciu o oryginalną kartę, autentyczne lub częściowo fikcyjne dane.

Przerobienie karty - w oryginalnych kartach zostają zmienione widniejące na nich dane. Występuje tu duża różnorodność sfałszowań. 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 zupełnie 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.

Fałszerstwo całkowite metodą białego plastiku(white plastic) - jest to odmiana opisanego wyżej podrobienia karty, która polega na naniesieniu na kartę różnych danych. Mogą to być elementy słowno-graficzne lub też tylko zapis na pasku magnetycznym. Ten typ przestępstwa często wymaga współdziałania przestępcy z osobami obsługującymi terminale POS. Białe karty również ułatwiają przestępcom wypłaty gotówki z bankomatu.

Fałszerstwo elektroniczne - to przestępstwo może polegać na posłużeniu się oryginalną kartą, która ma zmienioną zawartość paska magnetycznego. 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. Sprzedawca powinien zawsze sprawdzić, czy dane widniejące na rachunku są zgodne z danymi na karcie - w tym przypadku nie będą

Klonowanie pasków magnetycznych (skimming) - polega na wykorzystaniu nieuwagi posiadacza karty i skopiowaniu paska magnetycznego za pomocą specjalnego urządzenia, którego zdobycie nie sprawia żadnych problemów dla świata przestępczego. Urządzenie to wielkości kilku centymetrów bez problemu mieści się w dłoni. Wykorzystywane może być np. przez nieuczciwych sprzedawców w różnych punktach handlowo usługowych. [11]

Podsumowując powyższe rozważania, dojść można do wniosku, że posiadanie kart wiąże się ze znacznym ryzykiem osobistym, a popularność tego środka płatniczego spowodowana jest nie tylko korzyściami, lecz również niską świadomością społeczną tego zagrożenia. Ponad sto różnych istniejących technik przestępczych w tej dziedzinie, nie pozwala w pełni czuć się bezpiecznie ani przez moment. Metody te stają są coraz bardziej wyrafinowane, a stopień ich zaawansowania rozwija się wraz z rozwojem zabezpieczeń. Na szczęście, w ostatnim czasie duża część odpowiedzialności za utratę środków z konta klientów została przeniesiona na banki.

Cyber przestępstwa - hacking

Rozwój bankowości internetowej został ostatnio zachwiany, ujawnionymi i nagłośnionymi przez media, przypadkami skutecznego sabotażu internetowego. Przestępstwa te mogą w istotny sposób obniżyć poziom zaufania społecznego do bankowości elektronicznej i utrudnić jej dalszy rozwój. Niebywały wręcz rozwój techniki czy telekomunikacji w ostatnich latach dał przestępcom szeroką przestrzeń w jakiej mogą prowadzić swoją działalność. Możliwości teleinformatyczne, rosnąca komputeryzacja systemów łączności (w szczególności bankowych) uczyniła ten system „naczyń połączonych", bardzo narażonym na działalność cyber przestępców. Łatwe do przeprowadzenia ataki takie jak phishing czy pharming można szybko i skutecznie wykryć.

Wystarczy odpowiednia edukacja klientów, której banki starają się nie zaniedbywać. Motywuje to cyberprzestępców do obmyślania bardziej skomplikowanych metod wyłudzania poufnych danych. Jedną z nich jest w/w pharming, nazywany też zatruwaniem pamięci DNS (ang. DNS cache poisoning). Polega na przekierowaniu użytkownika Internetu do spreparowanej strony internetowej, która wyglądem może przypominać (lub być wręcz identyczna) witrynę banku internetowego, serwisu aukcyjnego, sklepu internetowego czy innej instytucji, która może przynieść hakerowi korzyści finansowe.

Aby przekierować internautę na sfałszowaną stronę logowania do konta bankowego, cyberprzestępcy nie muszą wysyłać mu żadnych specjalnych wiadomości. Wystarczy, że zmienią adresy DNS na komputerze lub serwerze ofiary, z której ta aktualnie korzysta. Podstawowym zadaniem systemu nazw domenowych jest przekształcanie adresów stron znanych internautom na adresy zrozumiałe dla urządzeń tworzących sieć komputerową. Istnieje kilka sposobów zatruwania pamięci DNS. Najbardziej rozpowszechniony polega na zarażeniu systemu ofiary odpowiednim koniem trojańskim. Kreatywność twórców szkodliwego oprogramowania zdaje się nie mieć granic. Specjaliści z firmy McAfee obliczyli, że codziennie pojawia się około 55 tys. nowych złośliwych aplikacji. [12] Inną metodą, zasługującą na uwagę jest driveby pharming. Jest to umiejscowienie w kodzie tworzonych przez cyberprzestępców stron, skryptów pisanych w języku JavaScript. Odnośniki do tych witryn są publikowane w serwisach społecznościowych, takich jak Facebook czy Twitter. Oszuści starają się też wypozycjonować je w wynikach wyszukiwania, używając do tego celu aktualnych, wzbudzających zainteresowanie tematów. Jeżeli internauta nabierze się i odwiedzi którąś z nich, zaimplementowany na stronie skrypt zmieni ustawienia DNS na jego routerze lub w punkcie dostępu bezprzewodowego. Może do tego dojść, jeśli router nie będzie chroniony hasłem albo hasło okaże się łatwe do odgadnięcia. [13] Aby skutecznie obronić się przed tego typu oszustwem należy przede wszystkim korzystać z usług zaufanego dostawcy internetu . Stosowane przez niego zabezpieczenia są pierwszą linią obrony na linii pharmingi-użytkownik. Nie należy też samemu zaniedbywać regularnego aktualizowania programu antywirusowego i zapory ogniowej (firewalla), które utrudnią koniom trojańskim przeniknięcie do komputera. Kolejnym krokiem jest włączenie automatycznych aktualizacji systemu Windows, niezałatane dziury są bowiem często wykorzystywane do zainfekowania komputera. Nie należy również zapominać o uaktualnianiu przeglądarki i zainstalowanych w niej wtyczek (w szczególności Flasha i Javy, których przestarzałe wersje są szczególnie podatne na ataki). Należy być przede wszystkim bardzo czujnym przy korzystaniu ze stron niewiadomego pochodzenia.

Uruchamianie na domowym komputerze stron z popularnymi portalami społecznymi, może wiązać się z ryzykiem, że zostały one w specjalny sposób spreparowane przez osoby zainteresowane pozyskaniem od nas informacji w sposób nielegalny.

Phishing (spoofing) to w branży komputerowej starszy brat pharmingu. Polega na wyłudzaniu poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej (S-E) czyli mówiąc ogólnie – naiwności użytkowników Internetu. [14] Termin ten jest niekiedy tłumaczony jako password harvesting fishing (łowienie haseł). Niektórzy znawcy utrzymują, że termin pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych, jeszcze w latach 80. Obecnie przestępcy sieciowi wykorzystują techniki phishingu w celach zarobkowych.

Do najpopularniejszych celów należą banki, instytucje finansowe czy aukcje internetowe. Oszust wysyła zazwyczaj spam do dużej liczby potencjalnych ofiar, kierując je na stronę w Sieci, która udaje rzeczywisty bank internetowy, a w rzeczywistości przechwytuje wpisywane tam przez ofiary ataku informacje. Typowym sposobem jest informacja o rzekomej dezaktywacji konta i konieczności ponownego jego reaktywowania, z podaniem wszelkich poufnych informacji. Strona przechwytująca jest łudząco podobna do prawdziwej, a powstałe zamieszanie było często potęgowane przez błąd w Internet Explorerze (w 2004 r. zajmował ponad 90% rynku przeglądarek), który pozwalał zamaskować także rzeczywisty adres fałszywej strony. Innym sposobem było tworzenie fałszywych stron pod adresami bardzo przypominającymi oryginalny, a więc łatwymi do przeoczenia dla niedoświadczonych osób. Przykład może stanowić phising jakiego dokonano podszywając się pod znany serwis zajmujący się płatnościami przez Internet - firmy Paypal. Hakerzy założyli wówczas stronę internetową wyłudzającą poufne informacje od użytkowników pod bardzo podobnym adresem www.paypai.com zamiast www.paypal.com. Liczba osób które dały się w ten sposób oszukać była liczona w tysiącach. Zastanawiająca jest w tym punkcie bezmyślności i naiwności ludzi, którzy nie zwrócili uwagi na podejrzany adres strony.

Czynnik ludzki, wspominany wcześniej podczas rozważań nad kartami płatniczymi, dotyczy również przestępstw komputerowych. Można również wysnuć wniosek, że jednym z kluczowych elementów łączących wszystkie rodzaje przestępstw opartych na fałszowaniu, jest naiwność ludzka w szerokiej postaci oraz zbytnie poczucie bezpieczeństwa w sytuacjach wymagających skupienia i rozwagi. Polski system prawny chroni użytkowników Internetu przed tego typu działalnością hakerów przewidując za takie działanie kary pozbawienia

wolności. Art. 267. § 1. kk RP mówi : kto 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, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Kodeks ten nie zawiera niestety rad, jak należy regularnie uaktualniać system i oprogramowanie, w szczególności klienta poczty e-mail i przeglądarkę WWW. O wszystkie te zabezpieczenia użytkownik musi zadbać sam. Dbałość o bezpieczeństwo w sieci, przy rosnącej licznie czynności jakie ludzie w niej wykonują, wymusić powinna na użytkownikach czujność oraz ograniczone zaufanie w trakcie pracy w Internecie.

W szponach sieciowej mafii

Liczba polskich internautów szybko rośnie. W roku 2006 do Sieci miało dostęp 36% Polaków, to trzykrotnie więcej, niż w roku 2000. Im więcej internautów, tym większe obroty sklepów internetowych, a co za tym idzie, większe zainteresowanie przestępców chcących zarobić na tego rodzaju przemyśle. Polacy coraz częściej wybierają zakupy przez Internet. Oszczędzają w ten sposób czas i pieniądze. Odnaleźć się w wirtualnym hipermarkecie i nie stracić głowy nie jest rzeczą prostą a aukcje internetowe to nie tylko komfort, ale i zagrożenie.

Najsłynniejszą techniką stosowaną przez oszustów jest podszywanie się pod sprzedającego. Technika oszusta polega na obserwacji aukcji w jej ostatniej fazie. Chwilę po zakończeniu licytacji wysyła on do wygrywającego wiadomość, w której przedstawia się jako sprzedawca i podaje numer swojego konta. Celem jest skłonienie kupca do wpłaty kwoty za przedmiot na konto oszusta. Należy pamiętać, że przelewów zagranicznych, podobnie jak krajowych, nie da się wycofać. Podczas zakupów w Sieci, zwłaszcza od sprzedawców spoza UE, często korzysta się z systemów płatności internetowych, takich jak PayPal utworzony przez eBaya. Niektóre z nich chronią kupującego, umożliwiając wycofanie już wykonanego przelewu, jeżeli towar nie dotrze do adresata. Jeśli nie mamy takiej możliwości, jesteśmy na łasce sprzedającego, gdyż potencjalne koszty prowadzenia procesu cywilnego za granicą najczęściej znacznie przekraczają wielkość spornej kwoty. Analogicznie odwrotną sytuacją jest gdy oszust będzie się podszywał pod osobę kupującą.[15]

Chciałbym na potrzeby tej pracy, przytoczyć wydarzenie, które jakiś czas temu miało miejsce w moim życiu. Po wystawieniu przedmiotu na aukcję internetową w jednym z popularnych polskich portali aukcyjnych, na mój adres mailowy zostało wysłane 3 listy z polskich kont pocztowych „pro konto” będących subadresami portalu o2.pl. Moją szczególną

uwagę zwrócił fakt, że w/w listy były napisane w języku angielskim, w sposób wskazujący na korzystanie z tłumacza. W milach trzy różne osoby pytały mnie, czy nie byłbym zainteresowany przesłaniem towaru poza terytorium Polski a dokładniej do Republiki Południowej Afryki. Po krótkiej wymianie korespondencji (bardzo intensywnej, co również wzbudziło moje podejrzenia biorąc pod uwagę opieszałość użytkowników tego typu portali), użytkownicy podali mi swoje adresy, dane kontaktowe nalegając na jak najszybsze wysłanie towaru. Moje pytania na temat przelewu pieniędzy były pomijane lub zdawkowo komentowane. Nie podając swojego numeru konta bankowego postanowiłem wyśledzić adresy IP komputerów z których maile zostały wysłane. Okazało się, że listy były wysyłane za pomocą serwera proxy i użytkownicy być może naprawdę pochodzili z RPA – tak wskazywały przynajmniej ich numer IP. Biorąc pod uwagę, że znaczna część osób korzysta z portali społecznościowych typu Facebook lub Twitter postanowiłem namierzyć te osoby w inny sposób - po informacjach podanych w mailu. Okazało się, że rzeczywiście istnieją tacy ludzie i mieszkają w jednym z miast w centrum RPA. Na pytania czy wysyłali do mnie listy w sprawie przedmiotu, odpowiedzi nie otrzymałem. W zamian za to po kilku chwilach na moją pocztę wpłynął list ponaglający mnie do wysłania przesyłki. Nie czekając długo, poinformowałem o wszystkim administratora portalu, a konta z których zostały wysłane listy, zostały natychmiast zablokowane. Po tym zdarzeniu oczywisty był wniosek, że obecny poziom inteligencji oszustów jest wprost proporcjonalny do misterności wykonywanych przez nich przedsięwzięć. Z opinii poznanych na fachowych forach dotyczących przestępstw cybernetycznych (c-crimes) dowiedziałem się, że nie byłem jedynym, któremu składano tego typu propozycje. Schemat działania przestępców był ten sam, w przypadku artykułów wszelkiego typu. To, że ich działalność nie została natychmiast ukrócona oznaczało, że organy ścigania miały naprawdę spory problem w namierzeniu tej szajki oszustów. Prawdą jest, że sposób w jaki profesjonalnie poruszali się w sferze sieciowej zacierając za sobą ślady, świadczyło, że są to osoby znające się doskonale na czarnej informatyce.

Podsumowanie pracy

W niniejszej pracy, poza dynamicznym rozwojem zjawiska fałszerstwa, pokazane zostały również słabe strony plastikowego pieniądza, handlu w sieci oraz transakcji pieniężnych. Mam wielką nadzieję, że nie zniechęci to czytelników, lecz wyczuli czujność na różnorakie zagrożenia. Niektóre rady zawarte tutaj mogą skutecznie utrudnić pracę oszustów. Korzystanie z dobrodziejstw współczesnej techniki powinno ułatwiać życie, jednak by tak się stało należy zwrócić uwagę na standardy bezpieczeństwa, które zapewnią należytą ochronę.

Od każdego indywidualnie zależy czy będzie mógł spać spokojnie nie drżąc o bezpieczeństwo swoich pieniędzy, danych osobowych itd. Przeciw wszechobecnym zagrożeniom powinno się podejmować wszelkie możliwe środki prewencyjne, gdyż dopiero one zapewnią wygodę i bezpieczeństwo.

---

[1] H. Kołecki, Technicznokryminalistyczne badania autentyczności dokumentów publicznych (praca zbiorowa), wyd. poznańskie, Poznań 2004, s. 9.

[2] L. Piniński, W 1400-letnią rocznicę kodyfikacji Justynina, Warszawa 1935 (cyt. za T. Karwowski, Badania przerobionych dokumentów, op.cit., s. 17).

[3] T. Karwowski, *Badania* przerobionych dokumentów, s. 18.

[4] Kodeks Karny RP [w] http://prawo.money.pl/akty-prawne/ujednolicone-akty prawne/kodeksy/kodeks;karny;z;dnia;6;czerwca;1997;r;,1997,88,553,DU,410.html.

[5] Aleksander Pruszak, Historie spektakularnych fałszerstw i rodzaje falsyfikatów, 15 stycznia, [w] http://www.nbportal.pl/pl/np/numizmatyka/vademecumkolekcjonera/falszerstwa/historie-spektakularnych-falszerstw-i-rodzaje-falsyfikatow

[6] Jean Deuve, Tajna Historia Podstępu w czasie II wojny światowej, wyd. Muza SA, Warszawa 2000, s.176.

[7] http://www.toparh.com.pl/index.php/katalogi-dokumenty-potwierdzajace-tozsamosc-rp.html

[8] http://www.dsb.pl/szkolenia/fa%C5%82szerstwa-dokument%C3%B3w-papierowych-i-elektronicznych

[9] Roman Łuczak, Ogólne aspekty fałszowania dokumentów [w] Człowiek i dokumenty, nr 1 wyd. PWPW, Warszawa 2006, s. 17.

[10] Europejskie Regulacje w dziedzinie własności przemysłowej – nowe wyzwania , pod red. Alicji Adamek, zeszyt nr 28.

[11] Materiały wewnętrzne Banku PKO SA

[12] http://di.com.pl/news/33151.html

[13] Symantec , http://di.com.pl/news/15883.html

[14] http://education.apwg.org/

[15] http://hacking.pl/pl/news-4689
Podejrzany_o_kilkadziesiat_wyludzen_przez_internet_zostal_zatrzymany.html

Autor Mateusz Sabaj Data 21.05.2011