Komisja
Nadzoru
Finansowego

Mateusz Górnisiewicz
Radosław Obczyński
Mariusz Pstruś

Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną

Poradnik klienta usług finansowych

CEDUR

CEDUR

PORADNIK KLIENTA USŁUG FINANSOWYCH

Mateusz Górnisiewicz
Radosław Obczyński
Mariusz Pstruś

BEZPIECZEŃSTWO FINANSOWE W BANKOWOŚCI ELEKTRONICZNEJ – PRZESTĘPSTWA FINANSOWE ZWIĄZANE Z BANKOWOŚCIĄ ELEKTRONICZNĄ

Warszawa 2014

Komisja Nadzoru Finansowego

Publikacja została wydana nakładem Komisji Nadzoru Finansowego

Pl. Powstańców Warszawy 1
00-030 Warszawa
www.knf.gov.pl

Warszawa 2014
Wydanie I

ISBN: 978-83-63380-63-2

Nakład: 5000 szt.

Stan prawny na dzień: 15 lipca 2014 r.

Przygotowanie do druku i druk:
Agencja Reklamowo-Wydawnicza A. Grzegorczyk
www.grzeg.com.pl

SPIS TREŚCI

WSTĘP

Rozwój bankowości elektronicznej, w tym dynamicznie rozwijającej się bankowości internetowej, opartej na elektronicznym przetwarzaniu danych, pociąga za sobą wzrost liczby różnorodnych form przestępczej aktywności wymierzonej przeciwko bezpieczeństwu danych, zagrażających bezpieczeństwu finansowemu na rynku usług bankowych, w szczególności bezpieczeństwu środków zgromadzonych na rachunku bankowym, do których dostęp możliwy jest na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych, takich jak komputer, telefon itp.

Nie ulega wątpliwości, że skala zagrożeń przestępczością w bankowości elektronicznej będzie wciąż rosła wraz z nieuniknionym, dalszym rozpowszechnianiem się usług bankowości elektronicznej, m.in. ze względu na coraz łatwiejszy do nich dostęp oraz atrakcyjność tych usług polegającą na wygodnym, niewymagającym osobistego udania się do banku, dostępie do środków zgromadzonych na rachunku bankowym, praktycznie nieograniczonym co do miejsca i czasu.

Nie można pominąć faktu, że na rozmiar przestępczości w elektronicznym obrocie bankowym ma również wpływ zachowanie indywidualnych uczestników rynku finansowego, którzy nie zawsze w dostatecznym stopniu są świadomi istniejących zagrożeń. Często nie posiadają też wiedzy o tym, jak mogą się przed nimi bronić.

Intencją autorów było stworzenie opracowania, którego celem będzie wzrost świadomości uczestników rynku finansowego w sferze zagrożeń związanych z korzystaniem z bankowości elektronicznej oraz upowszechnienie wiedzy na temat zasad postępowania, których przestrzeganie w znacznym stopniu pozwoli ustrzec się przed nimi, a także przybliżenie problematyki dotyczącej istoty i specyfiki przestępstw związanych z bankowością elektroniczną.

Niniejsza publikacja składa się z części koncentrującej się na praktycznym aspekcie problematyki związanej z bezpieczeństwem finansowym w elektronicznym obrocie bankowym oraz z części teoretycznej, w której przedstawione zostały podstawowe zagadnienia związane z bankowością elektroniczną i środowisko prawne, w którym ona funkcjonuje.

W rozdziale 1 zostały przedstawione w zrozumiały i przystępny sposób przykłady konkretnych naruszeń bezpieczeństwa finansowego w bankowości elektronicznej, z którymi może się zetknąć konsument uczestniczący w elektronicznym obrocie bankowym. Poszczególne przykłady zostały opatrzone teoretycznym komentarzem zawierającym opis zachowań, dzięki którym klient korzystający z bankowości elektronicznej może zapewnić sobie indywidualną ochronę przed zjawiskami zagrażającymi bezpieczeństwu finansowemu.

Praktyczne odwołanie do konkretnych kazusów ma także realizować walor edukacyjno-prewencyjny poprzez przybliżenie przed czym i w jaki dokładnie sposób indywidualni uczestnicy ryn-

ku finansowego mogą we własnym zakresie podjąć działania ochronne, które stanowią istotny czynnik decydujący o bezpieczeństwie finansowym. W tym kontekście istotne jest zrozumienie podstaw działania sieci oraz technik i narzędzi wykorzystywanych do popełniania przestępstw w bankowości elektronicznej.

Rozdział 2 został poświęcony przybliżeniu treści zasad zapewnienia bezpieczeństwa finansowego w bankowości elektronicznej.

Przestrzeganie bowiem podstawowych zasad bezpieczeństwa finansowego w bankowości elektronicznej jest w stanie zapewnić w znacznym stopniu skuteczną ochronę przed zagrożeniami związanymi z korzystaniem przez klientów banków z usług bankowości elektronicznej i obniżyć prawdopodobieństwo stania się ofiarą nadużyć dokonywanych w elektronicznym obrocie bankowym.

W rozdziale 3 zdefiniowane zostały ogólne pojęcia związane z bankowością elektroniczną, w tym podjęto próbę wskazania znaczenia pojęcia „przestępstwo związane z bankowością elektroniczną". Rozdział 4 zawiera natomiast analizę prawną wybranych czynów zabronionych, istotnych z praktycznego punktu widzenia omawianej problematyki.

Warto zwrócić uwagę na trudności dowodowe związane z procesem pozyskiwania i zabezpieczania dowodów elektronicznych w celu zapewnienia możliwości wykorzystania ich jako pełnowartościowych dowodów w postępowaniu przed sądem, wymagające uwzględnienia specyficznych właściwości tych dowodów, które wymuszają stosowanie odmiennych niż w przypadku tradycyjnych przestępstw zasad gromadzenia materiału dowodowego, opartych na fachowości i specjalistycznej wiedzy osób uczestniczących w czynnościach procesowych, w toku których dochodzi do zabezpieczenia śladów dowodowych w postaci elektronicznej.

Publikacja adresowana jest do szerokiego kręgu odbiorców, zarówno tych, którzy już korzystają z usług bankowości elektronicznej, jak i tych, którzy dopiero planują skorzystać z tego rodzaju usług.

Publikacja może okazać się również pomocna dla osób zajmujących się w praktyce przestępczością związaną z bankowością elektroniczną, w szczególności ze względu na omawianą w rozdziale 4 problematykę obejmującą analizę wybranych przepisów części szczególnej kodeksu karnego oraz zagadnień procesowo-kryminalistycznych związanych z pozyskiwaniem materiału dowodowego.

SŁOWNIK POJĘĆ

Certyfikat klucza publicznego – zestaw informacji, które w ogólnym przypadku nie są możliwe do podrobienia i które służą do weryfikacji tożsamości podmiotu w internecie.

EasyRecovery – program komputerowy pozwalający odzyskać utracone lub skasowane dane, pliki, foldery.

EMV – standard opracowany przez zrzeszenie wydawców kart płatniczych: Europay, MasterCard i Visa, definiujący zasady współpracy kart płatniczych wyposażonych w chip (tzw. chip EMV) z innymi urządzeniami, takimi jak terminale kartowe i bankomaty.

Hacking – zachowanie polegające na nieuprawnionym uzyskaniu dostępu do informacji w wyniku przełamania systemu zabezpieczeń.

Hot-spot – punkt dostępu do sieci bezprzewodowej, umożliwiający podłączonym do niego urządzeniom dostęp do internetu.

Informatyka śledcza – proces poszukiwania, zabezpieczania oraz analizy danych elektronicznych, którego celem jest dostarczenie dowodów elektronicznych spełniających określone kryteria dowodowe pozwalające na ich wykorzystanie w postępowaniu przed sądem.

Karta zbliżeniowa – karta płatnicza pozwalająca na dokonywanie autoryzacji transakcji poprzez przyłożenie do czytnika terminala płatniczego. Dla transakcji realizowanych w Polsce, o ile kwota transakcji nie przekracza 50 zł, nie jest zwykle wymagane podanie kodu PIN.

Kod CVC2/CVV2 – kod zapisany na odwrocie karty płatniczej pozwalający – wraz z numerem karty, datą jej ważności oraz danymi posiadacza karty – na przeprowadzanie transakcji typu „card-not-present".

Komisja Nadzoru Finansowego (KNF) – państwowy organ nadzoru, sprawujący nadzór nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym i emerytalnym, nad instytucjami płatniczymi i biurami usług płatniczych oraz nad spółdzielczymi kasami oszczędnościowo-kredytowymi i Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową; celem nadzoru nad rynkiem finansowym jest zapewnienie prawidłowego funkcjonowania tego rynku, jego stabilności, bezpieczeństwa oraz przejrzystości, zaufania do rynku finansowego, a także zapewnienie ochrony interesów uczestników tego rynku.

Modus operandi (dosł. sposób działania) – charakterystyczny dla danego sprawcy sposób działania.

Oprogramowanie szpiegujące (tzw. spyware) – programy komputerowe, których celem jest gromadzenie informacji o użytkowniku oraz przesyłanie danych i informacji użytkownika lub o użytkowniku bez jego wiedzy autorowi programu lub innej osobie.

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (np. danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań.

Płatności mobilne – płatności dokonywane przy użyciu telefonu komórkowego.

Procedura charge-back – procedura realizowana w związku ze zgłoszeniem przez klienta transakcji dokonanej kartą płatniczą do banku – wydawcy karty, np. w sytuacji nieotrzymania zakupionego towaru, w wyniku której następuje zwrot środków pieniężnych z rachunku sprzedawcy na rachunek kupującego.

Skimming – działanie przestępcze polegające na skopiowaniu przy użyciu urządzenia zainstalowanego np. na wlocie kart w bankomacie (tzw. skimmera) danych z paska magnetycznego karty płatniczej, co następnie umożliwia zdublowanie takiej karty.

Sniffer – program komputerowy wykorzystywany do przechwytywania i analizowania danych z sieci.

Sniffing (z j. ang. *węszenie*, *podsłuchiwanie*) – przechwytywanie przez nieuprawnione osoby informacji przesyłanych w lokalnych sieciach, a także sieciach WiFi.

Socjotechnika (również: inżynieria społeczna) – stosowanie różnorodnych środków psychologicznych i metod manipulacji w celu wyłudzenia od ofiary określonych informacji lub nakłonienia ofiary do realizacji określonych działań.

Spoofing – podszywanie się pod inny element systemu informatycznego, np. komputer innego użytkownika, w celu wykorzystania go jako narzędzia do dokonywania innych bezprawnych działań, np. do przeprowadzenia ataków na określone strony internetowe.

Suma kontrolna – unikatowa liczba obliczona według specjalnego algorytmu służąca do zapewnienia integralności danych.

Routery WiFi – urządzenia służące do bezprzewodowego udostępniania łącza internetowego.

Terminal POS (j. ang. Point of Sale – punkt handlowy) – urządzenie instalowane w punktach handlowo-usługowych służące do odczytywania danych z karty płatniczej oraz do kontaktowania się z centrum autoryzacyjnym, umożliwiające dokonanie płatności za nabywany towar lub usługę w formie bezgotówkowej (przy użyciu karty płatniczej).

Transakcja typu „card-not-present" – transakcje płatnicze realizowane bez fizycznej obecności karty u sprzedawcy, np. przez internet.

Urządzenia komutacyjne – urządzenia przewidziane do stosowania w sieci telekomunikacyjnej, odpowiedzialne za zestawianie połączeń telekomunikacyjnych.

Zapora sieciowa (ang. firewall) – oprogramowanie lub urządzenie służące do kontrolowania przepływu danych do i z danego urządzenia (np. komputera).

k.k. – ustawa z dnia 6 czerwca 1997 r. Kodeks karny.

k.p.k. – ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego.

CZĘŚĆ PRAKTYCZNA – ZASADY BEZPIECZNEGO KORZYSTANIA Z BANKOWOŚCI ELEKTRONICZNEJ

1. CO ZAGRAŻA NASZEMU BEZPIECZEŃSTWU W BANKOWOŚCI ELEKTRONICZNEJ I JAK SIĘ PRZED TYM BRONIĆ?

1.1 Wyłudzenia danych pozwalających na przeprowadzenie transakcji

Przykład

Po ciężkim dniu spędzonym w pracy zmęczony Pan Robert w końcu wsiadł do samochodu i ruszył w kierunku domu. Nagle usłyszał dzwonek telefonicznego zestawu głośnomówiącego.

– Dzień dobry Panie Robercie. Dzwonię z pańskiego banku w związku z realizowanym przez nas projektem, którego celem jest znaczące podniesienie poziomu bezpieczeństwa naszych klientów oraz deponowanych przez nich środków pieniężnych. W celu potwierdzenia pańskiej tożsamości, uprzejmie proszę podać swój login do bankowości internetowej.

– Bardzo proszę: robkow123.

– Dziękuję. Proszę jeszcze podać pierwsze sześć znaków pańskiego hasła.

– „L", „u", „b", „i", „e", „K".

– Niestety, coś się nie zgadza. Proszę w takim razie podać sześć ostatnich znaków.

– Przepraszam, musiałem coś pomylić. Ostatnie sześć znaków to: „i", „e", „K", „o", „t", „y".

– Dziękuję, już wszystko się zgadza. Jednym z elementów naszego projektu jest przeniesienie funkcji potwierdzeń SMS na nowoczesne, superbezpieczne serwery. W związku z tym, w celu przełączenia pańskiego konta na nowy serwer, za chwilę prześlemy panu SMS testowy. Proszę sprawdzić, czy tytuł przelewu testowego w SMSie to „SMS testowy – bezpieczne transakcje".

– Tak, zgadza się.

– Czy kwota operacji to 10 000 PLN?

– Tak.

– Doskonale, wygląda na to, że wszystko działa poprawnie. Już tylko jeden krok dzieli pana od pełnego zabezpieczenia pańskiego konta. W celu ostatecznej weryfikacji, proszę jeszcze tylko o podanie ośmiocyfrowego kodu zawartego w SMSie.

– Proszę bardzo: 01021418.

– Dziękuję, operacja przebiegła poprawnie. Teraz może pan spać spokojnie. Jeszcze raz dziękuję za współpracę i życzę miłego wieczoru.

Nastrój Pana Roberta bardzo się poprawił. W końcu to miło, że jego bank sam z siebie dba o wzmacnianie poziomu bezpieczeństwa jego pieniędzy. Po powrocie do domu postanowił jeszcze sprawdzić, czy w związku z „przełączeniem jego konta na nowy serwer" uległ zmianie wygląd serwisu jego bankowości internetowej. Po zalogowaniu okazało się jednak, że jedyne, co uległo zmianie, to stan jego konta – zostało ono bowiem uszczuplone o 10 000 złotych.

Zapamiętaj!

Żaden bank nigdy, pod żadnym pozorem nie prosi o podawanie żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z kart-zdrapek ani przesyłanych SMSem itp.), czy to telefonicznie, czy poprzez pocztę elektroniczną, czy w jakikolwiek inny sposób – poza serwisem internetowym bankowości elektronicznej i udostępnianymi przez banki aplikacjami (np. instalowanymi na telefonach komórkowych).

Jest to podstawowa zasada bezpieczeństwa korzystania z bankowości internetowej, o której zawsze należy pamiętać. O ile bowiem opisana powyżej historia Pana Roberta może wydawać się stosunkowo naiwna, o tyle przestępcy potrafią wymyślać bardzo zróżnicowane i wyrafinowane metody wyłudzania tego rodzaju danych. Niekiedy są to np. wiadomości e-mail (również rzekomo przesyłane przez bank), w których potencjalne ofiary proszone są o wprowadzenie kilkudziesięciu kodów jednorazowych z kart-zdrapek. Innym sposobem często wykorzystywanym przez przestępców jest przesyłanie w wiadomościach e-mail linków rzekomo prowadzących do serwisów bankowości internetowej, a w praktyce będących stronami internetowymi na serwerach przestępców, które zwykle do złudzenia przypominają te serwisy.

„Sposobem często wykorzystywanym przez przestępców jest przesyłanie w wiadomościach e-mail linków rzekomo prowadzących do serwisów bankowości internetowej, a w praktyce będących stronami internetowymi na serwerach przestępców, które zwykle do złudzenia przypominają te serwisy."

Użytkownik wprowadzając na takiej stronie swoje dane logowania oraz dane autoryzacyjne płatności w praktyce przekazuje je przestępcom. Taki rodzaj przestępczej działalności często nazywany jest **phishingiem**. Warto tu również zwrócić uwagę, że w celu zwiększenia skuteczności tego rodzaju działań przestępcy często stosują różnorodne metody manipulacji (co jest niekiedy nazywane socjotechniką lub inżynierią społeczną), takie jak

informowanie ofiar o „jedynej, niepowtarzalnej okazji", która za chwilę ucieknie ofierze „sprzed nosa", czy też opisywanie swoich przestępczych działań jako nakierowanych właśnie na rzekome zwiększenie bezpieczeństwa ofiary.

Zapamiętaj!

W celu zabezpieczenia się przed wyłudzeniem danych pozwalających na przeprowadzenie transakcji bankowości internetowej, należy bezwzględnie przestrzegać następujących zasad:

1) nigdy, pod żadnym pozorem nie należy podawać żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z kart-zdrapek ani przesyłanych SMSem itp.) w żadnym innym miejscu niż strona internetowa banku prowadzącego dany rachunek lub w udostępnianej przez niego aplikacji (np. instalowanej na telefonie),
2) wejście do serwisu bankowości internetowej powinno zawsze odbywać się poprzez wprowadzenie jego adresu w pasku przeglądarki – nie należy korzystać w tym zakresie z wyszukiwarek internetowych ani – w szczególności – z linków przesyłanych w otrzymanych wiadomościach e-mail,
3) przed zalogowaniem do serwisu bankowości internetowej zawsze należy sprawdzić, czy połączenie jest szyfrowane, tj. czy przed adresem strony znajduje się przedrostek „https://" (a nie „http://"), a obok niego widnieje symbol kłódki; dodatkowo należy kliknąć we wspomniany symbol kłódki i sprawdzić, czy nie pojawia się informacja o błędnym certyfikacie klucza publicznego.

1.2 Kradzieże z wykorzystaniem złośliwego oprogramowania

Przykład

„Uwaga! Ostateczne wezwanie do wpłaty.

Termin uregulowania należności minął w dniu 30 Lipiec 2013. Nie uregulowanie należności w wysokości 15 000 PLN do w ciągu 3 dni od otrzymania tej wiadomości spowoduje wpisanie Twojej firmy do bazy dłużników oraz oczekuj odpowiedzialności karnej. Szczegóły znajdź w załączonym pliku.

Po więcej informacji zadzwoń – 00960 555 12 45.

Z poważaniem,
Zespół Zarządzanie Długami Suriw".

W pewien poniedziałkowy poranek e-mail o takiej treści wybudził Pana Wojciecha skuteczniej niż jego ulubione espresso. Dbając o wizerunek swojej firmy, szybko pobrał załącznik do powyższej wiadomości i spróbował go otworzyć, nie zważając ani na łamaną polszczyznę, którą napisana była wiadomość, ani nawet na ostrzeżenia zgłaszane przez

zainstalowany na jego komputerze program antywirusowy. Ponieważ jednak na ekranie nic więcej nie pojawiło się, spróbował zadzwonić pod wskazany w wiadomości numer telefonu, którego nikt nie odbierał. Po przeprowadzeniu szybkiego rachunku sumienia uznał, że nikomu z żadnymi płatnościami nigdy nie zalegał, w związku z czym uznał całą sprawę za żart i zajął się zupełnie innymi sprawami – akurat miał w planach właśnie wykonanie kilku przelewów.

Jakież było jego zdziwienie, gdy po kilku dniach wszedł na swój rachunek bankowości internetowej z komputera żony i zobaczył, że saldo na jego koncie wynosi równe zero złotych, a w historii operacji widnieją przelewy na wysokie kwoty do osób, o których nigdy nie słyszał. Szybko udał się do placówki swojego banku, gdzie został poinformowany, że przelewy, które przekazywał (w swoim mniemaniu) do swoich kontrahentów w rzeczywistości trafiły zupełnie gdzie indziej i faktycznie na jego rachunku nie ma już środków. Zadzwonił do znajomego informatyka, który poinformował go, że jest to typowy sposób działania szkodliwego oprogramowania wykradającego pieniądze z kont klientów banków (teraz Panu Wojciechowi przypomniało się mgliście, że jego bank przesyłał mu wiadomości informujące o tego rodzaju zagrożeniach, on jednak – w ferworze codziennej walki o byt – skutecznie je ignorował). Natychmiastowa diagnoza komputera Pana Wojciecha przeprowadzona przez owego znajomego potwierdziła jego najgorsze przypuszczenia... Jego komputer padł ofiarą wirusa, a on sam został skutecznie okradziony przez przestępców.
Na domiar złego, z otrzymanego na koniec feralnego miesiąca rachunku telefonicznego wynikało, że Pan Wojciech wykonał krótkie połączenie z numerem premium na Malediwach, w wyniku czego musi uiścić dodatkową opłatę w wysokości kilkudziesięciu złotych. Wtedy przypomniał sobie, że numer telefonu, na który zadzwonił w związku z owym oszukańczym e-mailem faktycznie wyglądał nietypowo, on jednak nie zwrócił na to uwagi, chcąc jak najszybciej wyjaśnić sprawę rzekomo nieuregulowanej płatności.

Takie sytuacje, jak opisana powyżej, zdarzają się niestety coraz częściej. Przestępcy już dawno zorientowali się bowiem, że środowiska teleinformatyczne instytucji finansowych są z reguły bardzo dobrze zabezpieczone, w związku z czym zaczęli szukać innych rozwiązań, w których przy możliwie niskich nakładach pracy możliwe jest uzyskanie możliwie wysokiego prawdopodobieństwa przeprowadzenia skutecznego ataku. Takim rozwiązaniem okazały się być właśnie komputery (i inne urządzenia dostępowe, jak np. tablety czy telefony komórkowe) użytkowników bankowości internetowej, które często są zabezpieczone jedynie w ograniczonym zakresie lub nawet wcale.

Zapamiętaj!

Dlatego niezmiernie ważne jest, aby każdy użytkownik bankowości internetowej pamiętał o podstawowych zasadach bezpieczeństwa w tym zakresie:

1) do korzystania z bankowości internetowej należy zawsze używać znanych sobie, zaufanych urządzeń, nie zaś np. komputerów w kafejkach internetowych, na których ktoś

wcześniej mógł zainstalować szkodliwe oprogramowanie; nie należy również w tym celu łączyć się z obcymi punktami dostępowymi do sieci bezprzewodowych, jak np. publicznie dostępne hot-spoty,

2) urządzenia używane do korzystania z bankowości internetowej powinny zawsze być zabezpieczone poprzez aktualne oprogramowanie antywirusowe i zaporę sieciową (ang. firewall),

3) na urządzeniach tych należy również zawsze instalować najnowsze aktualizacje bezpieczeństwa, zarówno samego systemu operacyjnego, jak i innego oprogramowania (przeglądarek internetowych i ich wtyczek, oprogramowania biurowego itp.),

4) nie należy ignorować alertów bezpieczeństwa zgłaszanych przez oprogramowanie antywirusowe,

5) nie należy także korzystać z pirackiego oprogramowania – poza łamaniem przepisów prawa, często instalacja takiego oprogramowania wiąże się z ukrytym wprowadzeniem do urządzenia szkodliwego oprogramowania.

Stosowanie się do powyższych zasad znacząco obniża prawdopodobieństwo stania się ofiarą skutecznego ataku przeprowadzonego przy użyciu szkodliwego oprogramowania.

1.3 Kopiowanie kart płatniczych

Przykład

Pani Maria i Pan Wojciech wraz z dziećmi zdecydowali się w długi weekend majowy pojechać do Torunia, aby pokazać swoim potomkom to piękne miasto. Pogoda sprzyjała spacerom i korzystaniu z usług kawiarni na rynku toruńskim, których tam akurat nie brakuje. Pani Maria i Pan Wojciech przyzwyczajeni są do płacenia gotówką, więc i tym razem zdecydowali się podjąć drobną kwotę z bankomatu. Wybrali taki, który akurat był blisko rynku i poszli delektować się kawą i lodami w rodzinnej atmosferze.

Po paru miesiącach, zapomniawszy już o podróży do Torunia, Pani Maria przed zrobieniem zakupów w sklepie poszła ponownie do bankomatu w centrum handlowym. Tym razem okazało się, że mimo iż upłynęło ledwie parę dni od wypłaty pensji, żadnych pieniędzy na rachunku nie ma. Zatrwożona wróciła do domu, żeby sprawdzić operacje na koncie. Zobaczyła zaksięgowane parę wypłat z bankomatu w jednym z krajów w Ameryce Południowej, w której nigdy w życiu nie była, a na pewno nie w okresie ostatnich paru miesięcy.

„Przestępcy na bankomatach umieszczają urządzenia, dzięki którym zczytują dane z naszych kart."

Pani Maria i Pan Wojciech stali się ofiarami tzw. **skimmingu**. Przestępcy na bankomatach umieszczają urządzenia, dzięki którym zczytują dane z naszych kart.
Co do zasady nie zawsze korzystając z bankomatu możemy zorientować się, że ktoś go „ulepszył" na swoje potrzeby. **Aby skutecznie zczytać zawartość karty, przestępcy instalują nakładkę na otwór, w który wsuwamy kartę.** Tym sposobem skanują całą zawartość paska magnetycznego, którą następnie mogą nagrać na dowolny kawałek plastiku z paskiem magnetycznym lub przesłać elektronicznie do swoich kolegów w dowolnej części świata, aby oni to zrobili. **W niektórych bankomatach karta po włożeniu do bankomatu wsuwa się, jednocześnie wibrując. Mechanizm ten zabezpiecza nas przed skimmingiem** utrudniając w takim przypadku zczytanie danych z paska przez urządzenie zamontowane na bankomacie. Dodatkowo banki często montują „zęby" bądź inne plastikowe wypustki wokół otworu na kartę, aby uniemożliwić zamontowanie tam tzw. skimmera.

Jednak sama zawartość paska to za mało. Potrzebny jest przecież jeszcze PIN. Tutaj pomagają przestępcom dwie technologie. Montują nad klawiaturą listwy z miniaturową kamerą albo używają fałszywej klawiatury, którą przyklejają na tę prawdziwą. Dzięki temu możemy wpisać PIN i wypłacić pieniądze, a przestępcy wiedzą, jakie klawisze zostały naciśnięte.

Skimming najczęściej dotyka bankomaty w dobrych lokalizacjach turystycznych, nie zlokalizowane w oddziałach bankowych, do których jest swobodny dostęp, i z którego korzysta dużo ludzi. Nikogo wtedy nie dziwią ślady zużycia na bankomacie, które mogłyby wskazywać na jakąś podejrzaną działalność, ani fakt, że ciągle w okolicach bankomatu znajdują się ludzie.

Obecnie znaczna część klientów banków posiada karty z wbudowanym chipem mającym na celu ochronę przed pozyskiwaniem przez przestępców danych dotyczących karty.

Wiadomość, że karta posiada chip jest zapisana na pasku magnetycznym karty. Bankomat czyta tę informację i inicjuje tzw. **moduł EMV**, który porozumiewa się z chipem na karcie.

Wówczas na ekranie bankomatu wyświetla się komunikat o możliwym wydłużonym czasie oczekiwania na przeprowadzenie danej operacji, jak np. wypłata środków, w związku ze wspomnianym odczytem danych z karty.

Po zeskimowaniu karty z chipem przestępcy nie mogą jej użyć w bankomacie, który obsługuje moduł EMV, a takich jest w Polsce większość, jeśli nie wszystkie. Taki bankomat odczyta informacje o tym, że karta ma chip, poszuka go na zeskimowanej karcie i oczywiście nie znajdzie i nie przeprowadzi transakcji. Są jednak kraje, w których technologia EMV nie działa tak dobrze albo w ogóle (np. Ameryka Południowa czy USA). Tam komunikat o chipie z paska magnetycznego karty nie będzie zinterpretowany przez bankomat, a przestępcy mając zawartość paska magnetycznego karty i numer PIN bez przeszkód dokonają wypłaty.

Oczywiście banki chronią siebie i swoich klientów przed tym rodzajem przestępstw i bardzo często takie wypłaty blokują przed ich dokonaniem. Nie zawsze jednak pojedyncze transakcje uda się wychwycić, dlatego niezbędna jest czujność.

Uwaga!

Nie zalecamy korzystania z bankomatów, które nie są umiejscowione w oddziałach banków. Jeśli musimy skorzystać z bankomatu poza oddziałem, należy sprawdzić czy żadne jego części nie wyglądają „dziwnie", „jakby doklejone", „nadmiernie wystające" i niezintegrowane z całym bankomatem. Jeśli klawiatura sprężynuje przy wprowadzaniu PINu albo nawet odkleja się, należy transakcję przerwać. W razie jakichkolwiek wątpliwości lepiej skorzystać z innego bankomatu, a swoje podejrzenia zgłosić na infolinii banku.

1.4 Kradzieże związane z kartami zbliżeniowymi

Przykład

Rok akademicki nareszcie zakończył się! Robertowi wydawało się, że czekał na ten moment od wieków. Teraz poczuł, że życie jednak może być piękne. Zaliczona sesja, odłożone pieniądze zdobyte dzięki różnym zleceniom, które z zapałem realizował przez ostatnich kilka miesięcy – nareszcie można rozpocząć wymarzone wakacje. Z tą myślą – oraz z grupą najbliższych znajomych – Robert wsiadł do pociągu i już po kilku godzinach znalazł się nad polskim morzem. Plaża, wizyta w restauracji i nagle już widać wschodzące słońce. Takie wakacje mogłyby trwać cały rok!

„Hola hola, gdzie moja karta" – pomyślał Robert budząc się następnego dnia w okolicach południa i zaglądając do portfela. Niestety, nawet dogłębna inwentaryzacja wszystkiego, co tylko dało się zinwentaryzować, nie przyniosła dobrych dla Roberta rezultatów. Karty nie było nigdzie! Chcąc nie chcąc, Robert z wyjątkowo kwaśną miną musiał wykonać telefon w celu zastrzeżenia karty (na szczęście pamiętał **uniwersalny numer telefonu, pod którym 24 godziny na dobę i 7 dni w tygodniu można zastrzec swoją kartę płatniczą: +48 828 828 828**). Następnie swoje kroki skierował do placówki swojego banku, gdzie dokonał ze swojego rachunku wypłaty środków, które powinny pozwolić mu godnie przeżyć najbliższych kilka dni, a przy okazji dowiedział się, że z jego konta w tym czasie zniknęło niemal 600 PLN – było to kilkanaście transakcji zbliżeniowych poniżej 50 PLN, w przypadku których nie jest wymagane podanie kodu PIN. W pierwszej chwili ta kwota niemal zwaliła Roberta z nóg, na szczęście pani w okienku od razu poinformowała go, że w takiej sytuacji jego odpowiedzialność za utracone środki wynosi 50 EUR[1], musi tylko zgłosić stosowną reklamację i poczekać na jej pozytywne rozpatrzenie. Humor Roberta uległ dzięki temu minimalnej poprawie, a smaczne śniadanie w nadmorskiej karczmie niemal zupełnie rozwiało jego czarne myśli. Po powrocie do domu postanowił natomiast zgłębić temat bez-

[1] Zgodnie z art. 46 Ustawy o usługach płatniczych w przypadku dokonania nieautoryzowanych transakcji kartą płatniczą, odpowiedzialność płatnika wynosi 150 euro, gdy transakcja jest skutkiem kradzieży karty płatniczej. Jednocześnie zgodnie z dokumentem „Rekomendacje Rady ds. Systemu Płatniczego w zakresie bezpieczeństwa kart zbliżeniowych", odpowiedzialność użytkownika karty zbliżeniowej wynosi 50 EUR w przypadku, gdy bank – wydawca karty oferuje możliwość wyłączenia funkcjonalności płatności zbliżeniowych lub posiadanie karty bez takiej funkcjonalności, zaś w przeciwnym przypadku jest całkowicie wyłączona.

pieczeństwa kart zbliżeniowych – w tym celu zapoznał się z **opublikowanym przez Urząd Komisji Nadzoru Finansowego raportem „Analiza poziomu bezpieczeństwa kart zbliżeniowych z punktu widzenia ich posiadaczy"**, dostępnym na stronie Urzędu pod adresem: http://www.knf.gov.pl/Images/14_06_2013_karty%20zblizeniowe_tcm75-34934.pdf.

Karty zbliżeniowe to nowoczesna i wygodna forma płatności. Wbrew spotykanym niekiedy opiniom nie są one również mniej bezpieczne niż karty pozbawione funkcji zbliżeniowej. Należy bowiem zwrócić uwagę, że wprawdzie faktycznie utrata karty zbliżeniowej umożliwi przestępcy dokonanie za jej pomocą kilku transakcji, jednak odpowiedzialność klienta w tym zakresie jest ograniczona do maksymalnie 50 EUR.

„Działania przestępcze nakierowane są na kradzież danych z kart (zwłaszcza kredytowych) – niezależnie od tego, czy są one zbliżeniowe, czy nie – i dokonywanie nimi tzw. transakcji typu „card-not-present" (bez fizycznej obecności karty, np. przez internet)."

Dodatkowo warto zauważyć, że jednym z najistotniejszych problemów w zakresie kart płatniczych pozostają działania przestępcze nakierowane na kradzież danych z kart (zwłaszcza kredytowych) – niezależnie od tego, czy są one zbliżeniowe, czy nie – i dokonywanie nimi tzw. transakcji typu „card-not-present" (bez fizycznej obecności karty, np. przez internet).

W tym kontekście należy zwrócić uwagę, że dzięki użyciu technologii zbliżeniowej posiadacz karty w przypadku wielu transakcji nie musi tracić z nią fizycznego kontaktu, dzięki czemu ograniczane jest ryzyko sklonowania karty poprzez skimming lub nieuprawnionego odczytania z niej danych umożliwiających dokonanie transakcji typu „card-not-present".

Zapamiętaj!
W przypadku utraty karty niezwłocznie zgłoś ten fakt w placówce banku lub pod ogólnopolskim numerem telefonu +48 828 828 828.

1.5 Kradzieże przy użyciu danych karty płatniczej

Przykład

Krzysztof kończy w tym roku gimnazjum. Żeby ułatwić wszystkim życie, zakłada sobie konto w banku i dostaje kartę płatniczą, dzięki której będzie mógł korzystać z pieniędzy, których rodzice już nie będą musieli mu dawać do ręki. Jako że rodzice ufają Krzysztofowi, postanowili na wakacje wyrobić mu kartę kredytową podpiętą pod ich rachunek kredytowy w banku, żeby w razie nieprzewidzianej sytuacji miał się czym ratować.

Karta ta ucieszyła Krzysztofa niezmiernie, więc jej zdjęcie miało być pierwszym w albumie z pierwszych prawie dorosłych wakacji relacjonowanych na Instagramie.

Krzysztof jednak utracił zaufanie rodziców, kiedy w tym samym dniu, w którym zrobił zdjęcie karty i opublikował je na Instagramie, rodzice stracili wszystkie pieniądze z konta kredytowego.

Nie jest to wina Instagrama czy Facebooka czy innego medium społecznościowego.

Obecnie informacje publikowane w internecie pozostają tam na zawsze. Z pomocą tego środka komunikacji możemy znaleźć prawie wszystkie informacje, jakich potrzebujemy – poczytać książki w bibliotekach na całym świecie czy zobaczyć z bliska obrazy wielkich mistrzów. W internecie działają też przestępcy, dla których zdjęcie karty kredytowej wystarczy do „wyczyszczenia" nam konta. Nie jest to przesadnie trudne, gdyż wystarczy spisać dane z karty i posłużyć się nimi w sklepie internetowym za granicą. Ci, którzy płacą kartami w polskich i europejskich sklepach doskonale wiedzą, że do przeprowadzenia transakcji trzeba podać „kod zabezpieczający" znajdujący się na odwrocie karty. Więc w jaki sposób okradziono Krzysztofa, który sfotografował tylko front karty? Niestety są kraje, w których **kod CVC2/CVV2** (bo o nim mówimy), trzycyfrowy kod wydrukowany z tyłu karty obok miejsca na podpis, nie jest wymagany i do skutecznego przeprowadzenia transakcji wystarczy numer karty, data ważności i dane personalne na niej wytłoczone.

Przykład

Słynna jest już historia pewnej Pani, która po przejściu huraganu nad USA opublikowała na Facebooku zdjęcie karty, którą dostała od Amerykańskiego Czerwonego Krzyża, na której znajdowały się pieniądze dla niej, jako poszkodowanej w tej katastrofie. W ciągu paru minut od zamieszczenia zdjęcia pieniądze zostały wypłacone z konta, podobnie jak w przypadku naszego Krzysztofa.

Wszystkie dane dotyczące naszej karty musimy bezwzględnie chronić. Nie polega to tylko na powstrzymaniu się od robienia jej zdjęć i publikowaniu ich w internecie, ale też na tym, aby uważnie obserwować co robią z nią osoby, u których płacimy. Przy transakcjach w terminalu nie ma potrzeby, aby pracownik sklepu tę kartę odwracał, chyba że porównuje nasz podpis. Odpowiednio zlokalizowane kamery ochrony, skierowane na kasy (np. na stacjach benzynowych) mogą wtedy nagrać wszystkie dane potrzebne do wyczyszczenia naszego rachunku, jeśli pracownik kartę niepotrzebnie odwraca. Jeśli nie zamierzamy korzystać z karty w internecie – najlepiej wyzerować limit na te transakcje, co można zrobić w oddziale swojego banku, albo w ogóle zablokować ten kanał, na co niektóre banki pozwalają. Wszystkie pozostałe transakcje będą wymagały fizycznej obecności karty, ale w ten sposób nie będzie możliwe np. zagwarantowanie rezerwacji w hotelu, co może być uciążliwe dla osób podróżujących.

1.6 Zagrożenia dotyczące płatności mobilnych

Przykład

Anna nigdy nie miała pamięci do liczb. Dlatego pierwszą rzeczą, którą zrobiła po instalacji aplikacji pozwalającej na dokonywanie płatności mobilnych na swoim telefonie było zapi-

sanie kodu PIN do tej aplikacji na kartce i umieszczenie jej w etui aparatu. Dzięki temu – jak pomyślała – nie była już zagrożona nienawistnymi spojrzeniami sprzedawcy i osób stojących za nią w kolejce w momencie, w którym nerwowo próbowałaby przypomnieć sobie PIN i zapłacić za zakupy. I faktycznie – kilka razy dzięki tej swoistej „zapobiegliwości" udało jej się uniknąć blamażu. Jednak pewnego dnia padła ofiarą złodzieja, który wykorzystując chwilę nieuwagi Anny ukradł jej telefon wprost z kawiarnianego stolika. Początkowo nie była tą sytuacją zbyt zmartwiona (w końcu „to tylko telefon"), jakież jednak było jej zdziwienie, kiedy następnego dnia po zalogowaniu do swojego konta zobaczyła, że w ciągu ostatnich 24 godzin jej środki finansowe zostały uszczuplone o ponad 1000 złotych. Dopiero wtedy przypomniała sobie o zainstalowanej na telefonie aplikacji do płatności mobilnych (i o zapisanym w telefonie kodzie PIN) i błyskawicznie dezaktywowała funkcję dokonywania takich płatności.

Płatności mobilne to stosunkowo nowa forma dokonywania transakcji płatniczych. Dla wielu użytkowników wiąże się ona ze znaczącą wygodą – nie muszą bowiem nosić przy sobie portfela ani kart płatniczych, zaś operacji (zarówno w punktach sprzedaży, w bankomatach, jak i w internecie) mogą dokonywać wyłącznie przy użyciu aparatu telefonicznego. Jednakże – tak jak w przypadku każdej innej technologii płatniczej – bezpieczne korzystanie z tej formy płatności wymaga zapamiętania pewnych podstawowych zasad, które pozwolą na zabezpieczenie się przed grożącymi nam niebezpieczeństwami.

Zapamiętaj!

1) Telefon z zainstalowaną aplikacją do płatności mobilnych powinien mieć włączoną blokadę ekranu, której dezaktywacja powinna wymagać wprowadzenia hasła (lub w inny sposób była możliwa do dokonania jedynie dla prawowitego właściciela telefonu),
2) nie należy zapisywać hasła do aplikacji płatności mobilnych na kartce (lub innym nośniku), zwłaszcza przechowywanej wraz z telefonem,
3) hasło do telefonu powinno być inne niż do aplikacji płatności mobilnych; hasła te powinny również być trudne do odgadnięcia,
4) telefon używany do dokonywania płatności mobilnych powinien zawsze być zabezpieczony przez aktualne oprogramowanie antywirusowe,
5) na telefonie służącym do dokonywania płatności mobilnych należy zawsze instalować najnowsze aktualizacje bezpieczeństwa systemu operacyjnego,
6) oddając telefon do serwisu warto odinstalować aplikację płatności mobilnych,
7) niezwłocznie po utracie telefonu, na którym zainstalowana była aplikacja płatności mobilnych, należy zgłosić ten fakt w swoim banku.

A jak zapamiętać taki trudny do odgadnięcia kod PIN? To – wbrew pozorom – bardzo proste. Warto sobie przypomnieć, że na ekranowej klawiaturze numerycznej telefonu do cyfr od 2 do 9 przypisanych jest po kilka liter (np. cyfrze 2 odpowiadają litery „ABC", cyfrze 3 – „DEF" itd.). Mając na uwadze ten fakt, można ułożyć sobie jakiś łatwy do zapamiętania tekst (np. „lubię

bezpieczne płatności mobilne"), wziąć pierwsze litery z tego tekstu (dla naszego przykładu będą to litery „L", „B", „P" i „M"), wprowadzić ich „cyfrowy odpowiednik" jako hasło (w tym przypadku 5276) i... gotowe!

1.7 Kradzieże tożsamości

Przykład

Pani Ania chce uzyskać kartę kredytową z drobnym limitem, bo czasami poduszka finansowa się przydaje. Znalazła ofertę jednego z banków i aby nie tracić czasu kontaktuje się z nim telefonicznie. Konsultant wypytuje ją o wszystkie szczegóły: dane osobowe, miejsce pracy, zarobki, kto może te zarobki potwierdzić. Nic nie budzi wątpliwości Pani Ani, bo są to standardowe pytania, jakie bank zadaje, a przy małej kwocie nie wymaga zaświadczenia o zarobkach tylko potwierdzi je telefonicznie z pracodawcą. Pani Ania, aby nie tracić czasu, całą rozmowę z konsultantem przeprowadza w tramwaju linii 17, jadąc do pracy na 9 rano. Już po dwóch dniach Pani Ania cieszy się przyznanym limitem kredytowym.

Po pół roku Pani Ania decyduje się zwiększyć nieco limit na swojej karcie. Lecz tym razem bank jej mówi, że nie spłaca innych kredytów w innych bankach. Ale Pani Ania innych kredytów nigdy nie zaciągała.

Niestety, wśród osób podróżujących z Panią Anią w tramwaju linii 17 koło godziny 9 rano, znalazła się jedna nieuczciwa osoba, która całą rozmowę z konsultantem nagrała przy użyciu swojego telefonu komórkowego. Następnie wszystkie dane Pani Ani wykorzystała w paru bankach, zmieniając oczywiście tylko adres korespondencyjny, aby ofiara nie wiedziała co się dzieje. W księgowości w firmie Pani Ani też telefony z banków nie wzbudziły podejrzenia, bo przecież uprzedziła, że stara się o kartę i będą dzwonić.

Przy mniejszych kwotach, w zależności od zarobków klienta i jego zdolności kredytowej, banki nie muszą potwierdzać zarobków poprzez pisemne zaświadczenie o zarobkach.

Tym sposobem, jeśli nie chronimy swoich danych osobowych, mogą one zostać wykorzystane do zaciągania kredytów. Nie tylko jednak musimy uważać na podawanie naszych danych osobowych w zatłoczonych środkach komunikacji miejskiej. Niejednokrotnie niektóre osoby podają wszystkie swoje dane osobowe przy poszukiwaniu pracy. W odpowiedzi na nasze CV, fałszywy pracodawca kontaktuje się w celu ustalenia terminu rozmowy kwalifikacyjnej i z prośbą o wypełnienie bardzo szczegółowego kwestionariusza osobowego na stronie internetowej lub o przesłanie odpowiednich danych w pliku na adres e-mail. Na potrzeby procesu rekrutacji szczegółowe dane o nas nie są potrzebne. Należy wystrzegać się tego typu ofert, mimo że mogą być bardzo kuszące. Tak pozyskane dane niekoniecznie muszą służyć do wyłudzeń kredytów.

Uwaga!

Jeśli podamy numer naszego rachunku bankowego, wszystkie dane osobowe i numer telefonu komórkowego – przestępcy mogą wykorzystać te informacje do zakładania rachunków bankowych, które następnie są używane np. do przesyłania pieniędzy pochodzących z przestępstw. Wtedy stajemy się tzw. słupami, np. w procederze prania pieniędzy.

W kwestiach ochrony danych osobowych warto zapoznać się z informacjami opublikowanymi na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych, gdzie wyszczególniono sytuacje, w których podanie pewnych danych nie jest konieczne.

Oczywiście pozostaje kwestia „aktywacji" tego fałszywego rachunku, do czego potrzebny jest mały przelew z oryginalnego konta osoby, której dane wykorzystano. Można tego dokonać wykorzystując inne metody opisane w tej publikacji, bądź poprzez zainfekowanie naszego telefonu w sposób zdalny wirusem, dzięki czemu przestępcy uzyskają dostęp do SMSów, którymi autoryzujemy przelewy i logujemy się do swojego rachunku. A przelew na 1 złoty może przejść przez nas niezauważony.

Dane osobowe są wielkim dobrem, które musimy chronić, nawet wbrew naszemu wrodzonemu zaufaniu do innych ludzi, w szczególności do potencjalnych pracodawców. Wzmożona czujność jest wymagana w sytuacjach, gdy ktokolwiek chce, abyśmy podawali więcej informacji niż wydaje się nam to konieczne.

1.8 „Oszustwa nigeryjskie"

Przykład

„Jestem najbliższym współpracownikiem Jego Wysokości Księcia Mahammada III – zaczynał się e-mail, który Pan Marek otrzymał pewnego dnia rano – Ze względu na bardzo mało rozwinięty system bankowy w naszym kraju, potrzebujmy pomocy, aby środki prawowitego Króla przemieścić do Europy i ukryć przed juntą wojskową. Oczywiście pomoc zostanie wynagrodzona, 5% kwoty przelewu".

Pan Marek zapalił się do pomysłu, bo niby nie wiadomo ile tych pieniędzy trzeba przekazać, ale król mało ich nie ma, więc można liczyć na duży zysk. Po szybkiej wymianie korespondencji okazało się, że aby wszystko przebiegło prawidłowo, Pan Marek musi wnieść małą opłatę manipulacyjną, którą sobie zrekompensuje dość szybko paroma tysiącami dolarów, jakie przypadną mu z prowizji. Widząc już te pieniądze swoimi oczami (i właściwie już je wydawszy), Pan Marek wykonał przelew. Dalszego kontaktu już w tej sprawie nie było.

Niestety, takie wiadomości dość często wysyłane są drogą elektroniczną. Zazwyczaj ich treść napisana jest w języku angielskim i niewiele osób zwraca na nie uwagę. Niemniej są tacy, którzy widzą w tym procederze szanse na zarobienie pieniędzy w łatwy i szybki sposób. Taki system postępowania oszustów doczekał się osobnej penalizacji w nigeryjskim kodeksie karnym

(art. 419) ze względu na swoją powszechność. Pieniądze przekazane oszustom są nie do odzyskania. Co do zasady trzeba powiedzieć, że Pan Marek i tak miał szczęście. Odpowiadając na podobne e-maile i wikłając się w tego typu przedsięwzięcia można również narazić się na dużo większe problemy niż tylko utrata oszczędności.

Zapamiętaj!

Przyjęcie pieniędzy niewiadomego pochodzenia na swój rachunek bankowy i przekazanie ich dalej może być udziałem w większym oszustwie – praniu pieniędzy czy nawet finansowaniu terroryzmu. Bardzo często środki pieniężne przekazywane zgodnie z opisanym procederem mogą pochodzić z tzw. phisingu.

Należy pamiętać, by nie podejmować działań, które wydają się podejrzane i co do legalności których mamy wątpliwości. Udział w przekazywaniu środków pieniężnych według opisanego wyżej schematu, może skutkować podjęciem odpowiednich czynności przez prokuraturę oraz sąd, a następnie wymierzeniem kary.

1.9 Kradzieże w sklepach internetowych

Przykład

Pani Julia i Pan Adam znaleźli dawno poszukiwany okap kuchenny w jednym ze sklepów internetowych i to aż o 200 złotych tańszy niż w innych. Okazja, której nie można przepuścić. Towar został zamówiony i opłacony przelewem, ponieważ sklep nie wysyła towaru za pobraniem i jeszcze nie wdrożył płatności kartą ze względu na zbyt krótki okres swej działalności.

Zamówiony i opłacony towar oczywiście nigdy do kupujących nie dotarł.

Ofiarą takiego oszustwa może zostać każdy i to nie tylko poprzez dokonywanie zakupów w sklepach internetowych, ale również na portalach aukcyjnych. Sprawcy wykorzystują w tym przypadku przelewy na rachunki, płatności przy użyciu PayPal bądź podobnych rozwiązań. Czasami – czego nie jesteśmy świadomi – tak przelane pieniądze trafiają prosto na rachunek karty pre-paid, z której są natychmiast podejmowane. Za najbezpieczniejszą formę płatności w sklepach internetowych uznaje się płacenie kartą. W ten sposób, w razie gdybyśmy mieli dalsze problemy, możemy w swoim banku uruchomić procedurę tzw. charge-back.

Dzięki niej, organizacje specjalizujące się w zakresie rozwiązań płatniczych, jak VISA i Mastercard, zabezpieczają swoich klientów przed oszustwami. Po udowodnieniu bankowi incydentu oszustwa i wszczęciu wspomnianej wyżej procedury, to bank podejmuje działania mające na celu odzyskanie utraconych przez poszkodowanego pieniędzy z banku, w którym rachunek posiadają przestępcy.

„Dzięki procedurze charge-back organizacje specjalizujące się w zakresie rozwiązań płatniczych, jak VISA i Mastercard, zabezpieczają swoich klientów przed oszustwami. Po udowodnieniu bankowi incydentu oszustwa i wszczęciu wspomnianej wyżej procedury, to bank podejmuje działania mające na celu odzyskanie utraconych przez poszkodowanego pieniędzy z banku, w którym rachunek posiadają przestępcy."

Dlatego też w większości przypadków tylko sprawdzone sklepy oferują płatności kartami. Inną, bezpieczną formą dokonywania płatności za towar zakupiony w internecie może być płatność za pobraniem, lecz wtedy musimy przy kurierze otworzyć przesyłkę i wszystko dokładnie sprawdzić.

Proszę pamiętać, że dane podawane w systemach autoryzacyjnych instytucji płatniczych są bezpieczne, lecz pod żadnym pozorem nie wolno tych danych podawać w e-mailu bądź w inny sposób umożliwiający ich pozyskanie przez inne osoby.

Niestety, po raz kolejny należy powtórzyć, że zbyt duże okazje nie zdarzają się często a niska cena towaru pełnowartościowego powinna zwrócić naszą uwagę w negatywnym tego słowa znaczeniu. Płatności przelewami, czy przedpłaty należy realizować w sklepach o uznanej renomie lub takich, w których już kupowaliśmy z powodzeniem. Pozytywne komentarze w portalach aukcyjnych też nie zawsze są dla nas sprzymierzeńcem, ponieważ można je fałszować czy kupować, tak jak „lajki" na Facebooku. Zdrowy rozsądek jest kluczem do naszego bezpieczeństwa.

1.10 Co zrobić, gdy pieniądze znikną z rachunku bankowego w wyniku przestępstwa?

Mimo najwyższej staranności, ostrożności i stosowania wszystkich zasad opisanych w tej publikacji może zdarzyć się, że staniemy się ofiarami przestępstw, o których była mowa. Najważniejsze jest zachowanie czujności i weryfikowanie wyciągów z kont kart kredytowych, bądź uważne przeglądanie historii naszych rachunków. W chwili, w której zauważymy transakcje nie przeprowadzone przez nas, mimo zdenerwowania należy zachować spokój. Przed niezwłocznym poinformowaniem banku, należy ponownie sprawdzić wszystkie przeprowadzone transakcje i upewnić się, czy nie były one zrealizowane przez osoby nieuprawnione.

Zapamiętaj!

Najszybszą drogą poinformowania banku o podejrzeniu popełnienia przestępstwa jest złożenie reklamacji przez telefon, gdzie musimy wskazać transakcje nie przeprowadzone przez nas i oświadczyć, że nikomu nie udostępnialiśmy karty i jej numeru, jak również loginów i haseł do bankowości elektronicznej. W trakcie przyjmowania reklamacji, pracownik banku zastrzeże naszą kartę bądź zablokuje dostęp do bankowości elektronicznej, a bank rozpocznie procedurę wyjaśniania naszego zgłoszenia.

W zależności od przyjętej w danym banku praktyki, możemy być zobowiązani do złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa. Można tego dokonać dwojako: udać się na najbliższą nam komendę policji i złożyć ustnie takie zawiadomienie, z którego sporządzony zostanie protokół. Wtedy zostaniemy jednocześnie przesłuchani w charakterze pokrzywdzonego. Dlatego też należy mieć ze sobą wyciąg z karty bądź wydruk z historii rachunku, aby udokumentować naszą stratę. Zawiadomienie można również złożyć w formie pisemnej, przesyłając je do prokuratury rejonowej właściwej ze względu na nasze miejsce zamieszkania (właściwość tę można ustalić w internecie). Prokuratura prześle nasze zawiadomienie do właściwej komendy policji, do której i tak będziemy musieli zgłosić się w celu złożenia zeznań w charakterze pokrzywdzonego.

Niezależnie od tych działań, w miarę możliwości dobrze jest poinformować właścicieli sklepów lub innych placówek, w których użyto naszej karty albo które otrzymały nasze pieniądze. Dane adresowe większości firm można znaleźć w internecie. Niektórym poszkodowanym podjęcie opisanych działań może sprawić trudności w przypadku próby skontaktowania się z zagraniczną firmą ze względu na barierę językową.

Zazwyczaj duże firmy posiadają procedury postępowania w przypadku nieuprawnionego użycia karty i mogą pomóc w działaniach naszemu bankowi, który z pewnością zgłosi się do nich.

W przypadku, gdy przestępstwo zostało popełnione z wykorzystaniem naszej karty kredytowej lub płatniczej bądź ich numerów, należy udać się do placówki bankowej w celu złożenia tzw. polecenia charge-back (choć są również banki, które umożliwiają złożenie takiego polecenia przez telefon). Jest to procedura reklamacyjna przeprowadzana przez organizację specjalizującą się w rozwiązaniach płatniczych, jak Visa czy MasterCard, polegająca na tym, że w przypadku oszustwa pieniądze są nam zwracane przez bank, który we współpracy ze wspomnianą organizacją podejmuje działania w celu ich odzyskania. Należy pamiętać, że w niektórych bankach charge-back to osobna procedura niż reklamacja składana w razie oszustwa, a co więcej, nie jest ona popularna wśród klientów, co oznacza, że konsultanci nie zawsze muszą o niej wiedzieć. Należy pamiętać, iż w przypadku organizacji takich, jak Visa czy MasterCard, przysługuje nam prawo zgłoszenia oszustwa i domagania się uruchomienia procedury charge-back.

Ale najważniejszą zasadą postępowania w takiej sytuacji jest zachowanie spokoju. Wszyscy, z którymi będziemy mieli styczność chcą nam pomóc i rozumieją nasze trudne położenie. Po lekturze tej publikacji będziemy mieli rozległą wiedzę o tych rodzajach przestępstw i o sposobie postępowania, co pozwoli nam sprawnie poradzić sobie z tym przykrym zdarzeniem.

2. PODSTAWOWE ZASADY ZAPEWNIENIA BEZPIECZEŃSTWA FINANSOWEGO W BANKOWOŚCI ELEKTRONICZNEJ

Śledzenie zmian technologicznych przez konsumentów może być utrudnione ze względu na szybkość ich wprowadzania, co mogą wykorzystywać przestępcy w swojej działalności. Dlatego też ważne jest, abyśmy do wszystkich nowości podchodzili z rozwagą.

Celem niniejszej publikacji nie jest zniechęcanie do korzystania z nowych technologii – ułatwiają nam bowiem one życie na każdym kroku. Musimy natomiast mieć pewność, że rozumiemy podstawowe mechanizmy, które rządzą technologią przez nas używaną. Pracownicy banków, zarówno w oddziałach, jak i na infolinii, posiadają informacje, które mogą przysłużyć się naszemu bezpieczeństwu, dlatego należy z tej wiedzy korzystać.

Należy również pamiętać, że wraz z użytkowaniem nowych technologii przez klientów, niektóre systemy zabezpieczeń są rozwijane, a inne są wprowadzane zupełnie od nowa. Wynika to z konieczności dynamicznego reagowania na zagrożenia, które czasami są w praktyce nie do przewidzenia w momencie wprowadzania technologii na rynek. Dopiero użytkowanie nowych produktów przez klienta pokazuje, gdzie potencjalnie mogą wystąpić słabości w zabezpieczeniach.

Niemniej **żadne zabezpieczenia techniczne nie pomogą nam, jeśli sami nie będziemy stosować się do podstawowych zasad bezpieczeństwa**, których podsumowanie można znaleźć w dalszej części niniejszej publikacji.

2.1 Poufność

Wszystkie nasze dane zawarte w dowodzie osobistym pozwalają nas jednoznacznie zidentyfikować. Ujawnienie ich komukolwiek, za wyjątkiem osób uprawnionych, bardzo poważnie może zagrozić naszemu bezpieczeństwu. Skoro na podstawie tych danych możemy założyć rachunek bankowy czy otrzymać kredyt, to często dokładnie to samo będą mogli zrobić przestępcy podszywający się pod nas. **Nie powinno się podawać danych osobowych w miejscach, gdzie mogą one być podsłuchane lub zapisane przez inną osobę.** Dane te nie mogą być wysyłane do osób, których nie znamy – nieważne jak intratną ofertę pracy czy przyszłego biznesu dla nas rzekomo mają. Tak samo złym pomysłem jest umieszczanie ich w internecie, który niektórym kojarzyć się może jako medium zapewniające anonimowość. Niestety, tak nie jest. Nie mamy kontroli nad tym, kto ma tam dostęp do naszych danych i co dalej z nimi zrobi. Należy również pamiętać, że informacja raz umieszczona w internecie, nawet po jej usunięciu, dalej tam pozostaje. W powszechnym użyciu są narzędzia, które pozwalają na sprawdzenie historycznej zawartości poszczególnych stron internetowych.

To samo dotyczy wszystkich danych, z których korzystamy w celu logowania się do bankowości internetowej, czy też numerów naszych kart płatniczych bądź kredytowych. Wiele osób ma na szczęście pełną świadomość tego, że **w sytuacji utraty karty płatniczej** (w wyniku jej kradzieży, czy zagubienia) **należy ją jak najszybciej zastrzec**. Z drugiej jednak strony wiele osób nie ma

świadomości tego, że równie niebezpieczną sytuacją jest zrobienie zdjęć karcie i opublikowanie ich w internecie czy w jakikolwiek inny sposób podanie jej numeru osobom nieuprawnionym. Wiele transakcji może być bowiem przeprowadzonych bez fizycznej obecności karty, jedynie przy użyciu jej numeru (niekiedy nawet bez konieczności podania kodu bezpieczeństwa – tzw. CVC2/CVV2 – umieszczonego na odwrocie karty).

2.2 Spokój

Wiele schematów, o których pisaliśmy wcześniej bazuje na wykorzystaniu naszego zdenerwowania lub podekscytowania. Przestępcy będą próbowali nami manipulować wmawiając nam, że przedstawiana oferta zakupu jakiegoś towaru jest jedyna, niepowtarzalna i kończy się już za chwilę (wystarczy tylko wprowadzić na obcej stronie internetowej swoje dane do logowania do bankowości internetowej), że grożą nam ogromne kary finansowe i inne konsekwencje za nasze rzekome zaniechania (i dlatego musimy jak najszybciej pobrać załącznik do podejrzanego maila), czy też że zostaliśmy wytypowani jako najlepszy kandydat spełniający warunki najwspanialszej pod słońcem oferty pracy (i wystarczy jedynie, że podamy „przyszłemu pracodawcy" nasze szczegółowe dane osobowe i dokonamy przelewu na złotówkę). W takich sytuacjach często niewystarczająco zastanawiamy się, czy to, co robimy, nie przyniesie nam więcej szkody niż potencjalnego pożytku – zwłaszcza, że możemy już więcej takiej oferty nie dostać. I właśnie ten schemat myślowy wykorzystują przestępcy. Za każdym razem, gdy jesteśmy zdenerwowani bądź podekscytowani, nasze myśli nie idą tym torem, którym poszłyby normalnie. Chcemy działać szybko, aby jak najefektywniej rozwiązać problem czy doprowadzić daną sytuację do szczęśliwego finału. Wtedy właśnie możemy pominąć te sygnały ostrzegawcze, które w normalnej sytuacji byśmy zauważyli.

Dobrym rozwiązaniem jest zawsze na chwilę zatrzymać się. Zastopować wszechogarniającą potrzebę szybkiego działania, chęć „żeby szybko załatwić sprawę i mieć z głowy kolejny problem" i gonitwę myśli, która temu towarzyszy. Jeśli pozwolimy sobie na chwilę zatrzymania i spokoju, możemy zastanowić się i sprawdzić polegając na naszej wewnętrznej, zazwyczaj bardzo dobrej intuicji, czy aby wszystko jest w porządku.

2.3 Zdrowy rozsądek

Zaryzykujmy stwierdzenie, iż każdy w podejmowanych działaniach kieruje się zdrowym rozsądkiem. Jednakże w sytuacjach wzmożonego stresu postępujemy nierozważnie i zapominamy o podstawowych zasadach bezpieczeństwa.

Zazwyczaj nasze działania powinny być poparte wiedzą i temu ma służyć niniejsza publikacja.

Co więcej – zawsze, gdy mamy wątpliwości powinniśmy pytać, choćby dlatego, że zwykle większym wstydem jest dać się oszukać niż przyznać do niewiedzy, która jest przecież przez nas niezawiniona. Pracownicy banków są również od tego, aby dzielić się swoją wiedzą, ostrzegać klientów i ich informować. Tak, jak w Państwa interesie leży nie być oszukanym, tak samo w interesie banku jest aby Państwo nie zostali oszukani, bowiem niejednokrotnie oznacza to znaczne straty również po stronie banku.

Walka z oszustami i innymi przestępcami jest wspólnym zmaganiem instytucji finansowych i klientów.

Proszę również pamiętać, że wszystkie sytuacje, które wydadzą się nam dziwne, takie jak e-maile z banku, telefony z prośbą o potwierdzenie danych przez bank, w którym nie mamy rachunku, możemy zgłosić do oddziału swojego banku, co pomoże w wykryciu ewentualnego oszustwa.

2.4 Wiedza

Dużo już powiedzieliśmy o wiedzy. Warto jednak podkreślić, jak istotne jest to, żebyśmy wiedzieli z jakich technologii korzystamy, jak one działają, jakie są ich plusy i potencjalne zagrożenia. Oczywiście, w chwili wprowadzania nowych technologii są one gruntownie testowane, ale żadna z nich nie daje stuprocentowej gwarancji bezpieczeństwa. Jednak wszystkie instytucje wprowadzając nowe produkty czy technologie dbają o to, aby ich klienci byli dobrze poinformowani. Korzystajmy z tej okazji, czytajmy i starajmy się zapamiętać najistotniejsze zagrożenia, aby móc się ich ustrzec. W tym miejscu warto wspomnieć, że artykuły prasowe również mogą okazać się cenne, niemniej zazwyczaj nie są one pisane przez profesjonalistów i mogą zawierać przekłamania, niejednokrotnie istotne. Jeśli rzeczywiście jakaś istotna luka w zabezpieczeniach produktów bankowych zostanie wykryta, klienci zostaną o tym poinformowani przez bank, który ma również obowiązek taką lukę usunąć. Bezpieczeństwo klientów leży w dobrze pojętym interesie banku.

Wiedza o mechanizmach funkcjonowania bankowości elektronicznej oraz o potencjalnych zagrożeniach wynikających z jej korzystania pozwoli konsumentom ustrzec się przed działaniem przestępców.

CZĘŚĆ TEORETYCZNA – ZAGADNIENIA PRAWNE

3. PRZESTĘPCZOŚĆ W BANKOWOŚCI ELEKTRONICZNEJ – ZAGADNIENIA OGÓLNE

3.1 Zakres definicyjny przestępstw związanych z bankowością elektroniczną

Na początku należałoby wyjaśnić znaczenie pojęcia **bankowość elektroniczna**. Określenie granic zastosowania tego pojęcia wskaże jednocześnie obszar inkryminowanych zachowań. Trzeba również zwrócić uwagę na brak legalnej definicji bankowości elektronicznej.
Pojęcie usług bankowości elektronicznej funkcjonowało w przepisach ustawy z dnia 12 września 2002 r. o elektronicznych instrumentach płatniczych[2], które z dniem 7 października 2013 r. zostały uchylone ustawą z dnia 12 lipca 2013 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[3].
Brak jest również w doktrynie jednolitej definicji bankowości elektronicznej.
Ze względu na fakt, że jest to niezwykle pojemne sformułowanie, charakteryzujące się bogatą różnorodnością form realizacji, w literaturze przedmiotu, jak i w praktycznym obiegu, funkcjonuje wiele pojęć określających bankowość elektroniczną, w zależności od przyjętych kryteriów wyodrębniających szczególne cechy odmian bankowości elektronicznej, w tym przyjętych sposobów kontaktu klienta i banku oraz używanych w tym celu rozwiązań technicznych i technologicznych. I tak, tytułem przykładu można wskazać definicję, według której bankowość elektroniczną ujmuje się jako „ogół środków teleinformatycznych umożliwiających dostęp do rachunku bankowego, przy wykorzystaniu urządzeń elektronicznych, takich jak komputer, telefon (stacjonarny lub komórkowy), elektroniczne czytniki kart"[4] lub jako „system, w którym rozliczenia finansowe odbywają się bez obiegu mediów papierowych, komunikacja między bankiem a jego klientami oraz w obrębie samego banku odbywa się w drodze teletransmisji i wszelkie dane przechowywane i przetwarzane są w bazach danych systemu"[5].

Niezależnie od faktu, że pojęcie bankowości elektronicznej jest różnie ujmowane w literaturze przedmiotu, należy zwrócić uwagę, że **cechą wspólną tych definicji jest zapewnienie dostępu do środków zgromadzonych na rachunku i możliwości dokonywania na nim operacji bankowych na odległość.** Nie jest więc konieczne fizyczne stawienie się w placówce banku, a dostęp do środków zgromadzonych na rachunku można uzyskać zasadniczo w każdej chwili i w dowolnym miejscu.

---

[2] Dz.U. z 2012 r. poz. 1232.
[3] Dz.U. z 2013 r. poz. 1036.
[4] B. Świecka, *Bankowość elektroniczna*, Warszawa 2004, s. 8.
[5] W. Chmielarz, *Systemy elektronicznej bankowości i cyfrowej płatności*, Warszawa 1999, s. 25.

„Bankowość elektroniczna jest pojęciem mającym rozległy zakres zastosowania, obejmującym szerokie spektrum elektronicznych form kontaktu, wśród których wyodrębnić można bankowość internetową, home-banking, telefoniczną, samoobsługową oraz inne kanały dostępu do konta (np. poprzez telewizję)."

Jak wynika z opisanych wcześniej definicji, bankowość elektroniczna jest pojęciem mającym rozległy zakres zastosowania, obejmującym szerokie spektrum elektronicznych form kontaktu wśród których wyodrębnić można, bankowość internetową, home-banking, telefoniczną, samoobsługową oraz inne kanały dostępu do konta (np. poprzez telewizję).

Bankowość internetowa, często niesłusznie utożsamiana z bankowością elektroniczną, jest najmłodszą i najbardziej gwałtownie rozwijającą się gałęzią bankowości elektronicznej.

Należy zauważyć, że termin **bankowość internetowa** mieści się w zakresie definicyjnym bankowości elektronicznej i **jest pojęciem węższym niż pojęcie bankowości elektronicznej**. Bankowość internetowa nie obejmuje swoim zakresem, jak to ma miejsce w przypadku bankowości elektronicznej, form kontaktu banku z klientem, które nie opierają się na wykorzystaniu ogólnodostępnej sieci internet, jak np. usługi bankowości mobilnej opartej na użyciu specjalnych aplikacji dostępnych dla telefonów komórkowych.
Za nieuprawnione zatem trzeba uznać próby zamiennego posługiwania się wyżej wymienionymi pojęciami.

Podkreślić należy, że brak jest definicji legalnej bankowości internetowej oraz że przepisy prawa nie posługują się tym pojęciem.
Termin bankowość internetowa wpisał się za to wyraźnie w kanon praktyki bankowej, która powszechnie posługuje się tym terminem we wzorach umów[6].
Podejmując próbę stworzenia definicji bankowości internetowej należy skoncentrować się na wskazaniu zasadniczych cech charakteryzujących to stosunkowo młode zjawisko.
Zacząć należy od stwierdzenia, że udostępnienie posiadaczowi rachunku bankowego bankowości internetowej następuje na podstawie umowy rachunku bankowego.
Dostęp do bankowości internetowej następuje przy pomocy standardowych urządzeń i oprogramowania umożliwiających dostęp do stron internetowych oraz opiera się na komunikacji za pośrednictwem portalu internetowego danego banku.
Dostęp do bankowości internetowej, tj. do określonych funkcji portalu internetowego banku oraz inicjowanie rozliczeń jest możliwe jedynie po spełnieniu przez posiadacza rachunku bankowego warunków identyfikacji i uwierzytelnienia ustalonych z bankiem w umowie.
Za pośrednictwem bankowości internetowej posiadacz rachunku bankowego może skorzystać z dwóch zasadniczych funkcji, tj. udostępnienia mu przez bank informacji o rachunku (np. o saldzie lub historii rachunku) oraz przekazania bankowi poleceń rozliczeniowych[7].

[6] W. Iwański, *Umowa rachunku bankowego objętego bankowością internetową z punktu widzenia nowej regulacji usług płatniczych*, Warszawa 2014, s. 50.
[7] Ibidem, s. 51.

Zapamiętaj!

Uwzględniając powyższe cechy należy stwierdzić, że bankowość internetowa to oparta na umowie usługa, na podstawie której właściwie zidentyfikowany posiadacz rachunku bankowego uzyskuje za pośrednictwem ogólnodostępnej sieci internet oraz standardowych urządzeń, dostęp do portalu internetowego banku, w ramach którego bank udostępnia informacje o rachunku i zapewnia posiadaczowi rachunku możliwość składania poleceń rozliczeniowych.

W przypadku usług home-bankingu[8] łączność z bankiem odbywa się poprzez sieć internetową lub telefoniczną i wymaga zainstalowania na komputerze klienta dedykowanego oprogramowania. Koszty funkcjonowania home-bankingu, wyższe niż w przypadku zyskującej coraz bardziej na popularności bankowości internetowej, zmniejszają zainteresowanie tego rodzaju usługami. Natomiast zaletą jest to, że program używany do przeprowadzania operacji może integrować się bezpośrednio z innymi programami używanymi w przedsiębiorstwie, ma rozbudowany system prezentacji umożliwiający przedstawienie analiz i raportów, pozwala na korzystanie z baz danych działających w programie.

„W przypadku usług home-bankingu łączność z bankiem odbywa się poprzez sieć internetową lub telefoniczną i wymaga zainstalowania na komputerze klienta dedykowanego oprogramowania."

Bankowość telefoniczna może być realizowana w formie phone banking lub mobile banking.
W przypadku phone banking klient łączy się z operatorem, który przyjmuje i wykonuje składane przez klienta zlecenia. Drugim sposobem jest automatyczna obsługa klienta z wykorzystaniem jednostronnej komunikacji głosowej, która polega na tym, że klient na podstawie otrzymywanych komunikatów głosowych wybiera interesującą go opcję za pomocą klawiatury telefonu.

„Bankowość telefoniczna może być realizowana w formie phone banking lub mobile banking."

Bankowość telefoniczna może być również realizowana przez wykorzystanie telefonów komórkowych lub innego urządzenia przenośnego (mobile banking). Polegać to może na wykorzystaniu komunikatów SMS do otrzymywania informacji lub potwierdzenia zdarzeń dotyczących rachunku bankowego lub wydawania tą drogą poleceń. W zakresie tego rodzaju bankowości mieści się również dostęp do rachunku bankowego z wykorzystaniem przeglądarek internetowych zainstalowanych w telefonie komórkowym.

Bankowość samoobsługowa (selfbanking) opiera się głównie na wykorzystaniu urządzeń zewnętrznych takich, jak terminale POS oraz bankomaty. Elektroniczny terminal POS służy do odczytywania danych z karty płatniczej oraz do kontaktowania się z centrum autoryzacyjnym.

[8] D. Cyman, *Elektroniczne instrumenty płatnicze a bezpieczeństwo uczestników rynku finansowego*, Warszawa 2013, s. 97-98.

Jako środek służący do kontaktowania się banku z klientem wykorzystywana jest również telewizja cyfrowa, chociaż obecnie nie odgrywa ona istotnej roli ze względu na ograniczoną dostępność tych usług.

Zgodnie z art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[9] *przez świadczenie usług drogą elektroniczną należy rozumieć wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.*
Sieć telekomunikacyjna w rozumieniu art. 2 pkt 35) ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne[10] to *systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.*

Przez pojęcie bankowości elektronicznej należy rozumieć formę usług świadczonych przez banki na rzecz klientów, polegającą na umożliwieniu dostępu do rachunku bankowego na odległość za pomocą urządzeń do elektronicznego przetwarzania i przechowywania danych takich jak komputer, telefon, bankomat, terminal, odbiorniki telewizji cyfrowej.

Przepisy prawa karnego nie określają definicji przestępstwa. Można ją natomiast wyprowadzić z przepisów części ogólnej ustawy z dnia 6 czerwca 1997 r. Kodeks karny[11], zwany dalej „k.k.", w tym w szczególności z art. 1, który stanowi, iż:

§ 1. Odpowiedzialności karnej podlega ten tylko, kto popełnia czyn zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia.
§ 2. Nie stanowi przestępstwa czyn zabroniony, którego społeczna szkodliwość jest znikoma.
§ 3. Nie popełnia przestępstwa sprawca czynu zabronionego, jeżeli nie można mu przypisać winy w czasie czynu.
Zgodnie z art. 115 § 1 k.k. *Czynem zabronionym jest zachowanie o znamionach określonych w ustawie karnej.*

[9] Dz.U. z 2013 r. poz. 1422.
[10] t.j. Dz.U. z 2014 r., poz. 243.
[11] Dz.U. z 1997 r., Nr 88, poz. 553 z późn. zm.

Uwzględniając powyższą definicję przestępstwa oraz wskazany wyżej zakres znaczeniowy pojęcia bankowość elektroniczna należy stwierdzić, że przestępstwo związane z bankowością elektroniczną to czyn o znamionach odpowiadających opisowi ustawowemu określonego typu czynu zabronionego pod groźbą kary, bezprawny, karygodny, zawiniony, popełniony w elektronicznym obrocie bankowym opartym na płatnościach bezgotówkowych i elektronicznym przetwarzaniu danych.

Analiza treści przepisów części ogólnej kodeksu karnego odnoszących się do odpowiedzialności karnej, w tym cytowanych wcześniej przepisów pozwala uznać, że przestępstwem jest czyn człowieka (zachowanie, przez które należy rozumieć zarówno działanie, jak i zaniechanie) o znamionach określonych w ustawie karnej, zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia, bezprawny, karygodny, zawiniony.

Czyn zabroniony pod groźbą kary przez ustawę (czyn karalny) to taki, który odpowiada opisowi ustawowemu określonego typu czynu zabronionego pod groźbą kary, tzw. ustawowemu wzorcowi.
Czyn bezprawny to taki, który naraża na niebezpieczeństwo lub narusza dobro chronione prawem i jednocześnie nie zachodzą okoliczności uzasadniające takie narażenie lub naruszenie, wynikające z konfliktu dóbr chronionych prawem, usprawiedliwiające poświęcenie danego dobra prawnego celem ratowania innego, ważniejszego dobra.
Czyn karygodny to czyn społecznie szkodliwy w stopniu wyższym niż znikomy.
Czyn zawiniony jest wówczas, gdy jego sprawcy można przypisać winę w czasie czynu.

3.2 Przestępstwa związane z bankowością elektroniczną w polskim systemie prawnym

Należy wskazać, że w przepisach polskiego prawa karnego nie istnieje jeden odrębny katalog przestępstw odnoszących się tylko do bankowości elektronicznej.

Na gruncie polskiego ustawodawstwa karnego przestępstwa związane z bankowością elektroniczną nie stanowią odrębnej kategorii czynów karalnych. Brak jest także odrębnego rozdziału w kodeksie karnym, który byłby poświęcony tylko tego rodzaju przestępstwom.
Nie oznacza to, że przestępcze formy zachowania związane z wykorzystaniem w elektronicznym obrocie bankowym nowoczesnych technologii teleinformatycznych opartych na przesyłaniu danych elektronicznych, pozostają poza zakresem penalizacji na gruncie polskiego prawa karnego, i że sprawcy tych czynów nie poniosą odpowiedzialności karnej.

Trzeba w tym miejscu również zaznaczyć, że wykorzystanie na rynku usług bankowości elektronicznej wspomnianych wyżej technologii, w tym sieci internet oznacza, że przestępstwa popełniane w elektronicznym obrocie bankowym wpisują się w szeroki nurt przestępczej aktywności zwanej **cyberprzestępczością**.

W polskim ustawodawstwie karnym brak jest definicji legalnej pojęcia cyberprzestępczość.
W ustaleniu definicji cyberprzestępczości może natomiast okazać się pomocna analiza treści preambuły zawartej w Konwencji Rady Europy o cyberprzestępczości[12] z dnia 23 listopada 2001 r., której stroną jest również Polska. Na marginesie należy jedynie dodać, że w celu implementowania do prawa polskiego przepisów Konwencji o cyberprzestępczości znowelizowane zostały odnośne przepisy kodeksu karnego, w tym w szczególności zawarte w rozdziale XXXIII k.k. zatytułowanym *Przestępstwa przeciwko ochronie informacji.*
We wspomnianej preambule czytamy m.in., że celem Konwencji jest powstrzymanie *działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo.*

Przez określenie cyberprzestępczość należy zatem najogólniej rozumieć czyny zabronione pod groźbą kary przez ustawę dokonywane przeciwko bezpieczeństwu systemów informatycznych, sieci, elektronicznie przetwarzanych danych, jak również przy użyciu tych systemów, sieci i danych.

Uwzględniając powyższe uwagi, należy stwierdzić, że przestępstwa związane z bankowością elektroniczną będą realizowały przede wszystkim znamiona ustawowe ogólnych typów czynów zabronionych określonych w przepisach części szczególnej kodeksu karnego, w szczególności w rozdziale XXXIII k.k. zatytułowanym *Przestępstwa przeciwko ochronie informacji.* Zachowanie sprawcy może także wypełniać ustawowe znamiona innych czynów zabronionych stypizowanych w przepisach zawartych m.in. w rozdziale XXIII k.k. zatytułowanym *Przestępstwa przeciwko wolności* np. w art. 190 a § 2 k.k., czy też w rozdziale XXXV k.k. zatytułowanym *Przestępstwa przeciwko mieniu* np. w art. 287 k.k. (oszustwo komputerowe).

Należy zauważyć, że katalog czynów zabronionych popełnianych w bankowości elektronicznej nie ogranicza się do przestępstw kodeksowych, bowiem odpowiedzialność karna może wynikać również z ustaw szczególnych, np. jeżeli w związku z elektronicznym przetwarzaniem danych w obrocie bankowym dojdzie do naruszenia ustawowo chronionej tajemnicy np. tajemnicy bankowej, zastosowanie znajdzie art. 171 ust. 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[13] przewidujący odpowiedzialność karną za nieuprawnione ujawnienie lub wykorzystanie informacji stanowiących tajemnicę bankową.

[12] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=25/06/04&CL=ENG
[13] t.j. Dz.U. z 2012 r., poz. 1376 z późn. zm.

4. PRZESTĘPSTWA ZWIĄZANE Z BANKOWOŚCIĄ ELEKTRONICZNĄ

4.1 Charakterystyka poszczególnych typów przestępstw

Z uwagi na znaczną rozpiętość form działania przestępczego w elektronicznym obrocie bankowym w dalszej części niniejszej publikacji zostaną szerzej omówione czyny zabronione mające istotne znaczenie praktyczne, w tym w szczególności związane z usługami bankowości internetowej wykorzystującej nowoczesne technologie, które generują nowe zagrożenia i których skala będzie wciąż rosła, ze względu na dalszy dynamiczny rozwój sieci internet i związany z tym powszechny do niej dostęp zapewniający anonimowość osobom działającym w sieci, w tym również przestępcom.

Bankowość internetowa jest zjawiskiem stosunkowo młodym, ale gwałtownie rozwijającym się. Z uwagi na fakt, że zapewnia wygodny i łatwy dostęp poprzez internet do środków zgromadzonych na rachunku bez konieczności osobistego udania się do placówki banku, należy spodziewać się, że wraz z dalszym upowszechnianiem dostępu do sieci internet, tendencję wzrostową będzie można nadal obserwować również na rynku usług bankowości internetowej.
Uwzględniając powyżej wskazane kryteria, w kolejnym punkcie omówione zostaną, w odniesieniu do bankowości elektronicznej, przestępstwa stypizowane w części szczególnej kodeksu karnego w następujących przepisach: w art. 267 k.k., art. 268 § 1 i § 2 k.k., art. 268a § 1 k.k., art. 286 § 1 k.k, art. 287 § 1 k.k. oraz art. 190 a § 2 k.k.

Powyższe przepisy penalizują m.in. takie formy przestępczych zachowań jak: wyłudzenia danych dotyczących karty płatniczej (np. w sklepach internetowych), konta internetowego, pozwalających na przeprowadzenie transakcji bankowych przez osoby nieuprawnione, a także nielegalne przechwytywanie wyżej wymienionych danych w czasie transmisji w środowisku elektronicznym, w tym również z wykorzystaniem złośliwego oprogramowania, tzw. kradzież tożsamości, zakładanie na bankomatach urządzeń do nielegalnego zbierania informacji z karty płatniczej będące częścią przestępczej działalności określanej jako **skimming**, bezprawne wykorzystywanie przez osoby nieuprawnione danych dotyczących karty płatniczej, konta internetowego, „oszustwa nigeryjskie".

4.1.1 Formy działania przestępczego

Art. 267 k.k.
§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.
§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Przedmiotem ochrony objętej zakresem penalizacji przewidzianej w cytowanym powyżej przepisie jest prawo do wyłącznego dysponowania określoną informacją przez osobę do tego uprawnioną. Ochroną, na podstawie art. 267 § 1 k.k., objęte są wszelkie informacje, w tym dane osobowe, hasła komputerowe, kody dostępu.

Do realizacji czynu określonego w art. 267 § 1 k.k. dochodzi poprzez **nieuprawnione uzyskanie dostępu do informacji**, które **może nastąpić poprzez**:

- otwarcie zamkniętego pisma,
- podłączenie się do sieci telekomunikacyjnej,
- przełamanie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia,
- ominięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia.

Uzyskanie dostępu do informacji nie oznacza spełnienia wymogu zapoznania się z treścią informacji. Za uznanie przestępstwa, określonego w art. 267 § 1 k.k., wystarczy samo tylko uzyskanie dostępu do informacji, nie jest konieczne zapoznanie się z jej treścią. Nieistotne jest zatem z punktu widzenia realizacji wyżej wymienionego czynu, czy sprawca zapoznał się z treścią informacji, czy wykorzystał ją do własnych celów, w szczególności do osiągnięcia korzyści majątkowej, lub czy ją jedynie zniszczył powodując w ten sposób szkodę, ale nie uzyskując korzyści majątkowej. W przypadku gdy sprawca nie zapoznał się z treścią informacji uzyskanej w którykolwiek ze sposobów określonych w § 1, 2 lub 3 analizowanego przepisu, ale przekazał ją innej osobie, wówczas dojdzie do realizacji ustawowych znamion czynu określonego w § 4 omawianego przepisu.
Przez przełamanie zabezpieczenia należy rozumieć każdą czynność bezpośrednio ingerującą w istniejące zabezpieczenia, która ma doprowadzić do uzyskania dostępu do informacji. Do przełamania zabezpieczenia nie wystarczy sama jego instalacja. Konieczne jest bowiem, aby w chwili działania sprawcy zabezpieczenie było aktywne i w konsekwencji doszło do jego przełamania.

„Zachowanie polegające na nieuprawnionym uzyskaniu dostępu do informacji w wyniku przełamania systemu zabezpieczeń w powszechnym obrocie funkcjonuje pod pojęciem **hackingu**.*”*

Zachowanie polegające na nieuprawnionym uzyskaniu dostępu do informacji w wyniku przełamania systemu zabezpieczeń w powszechnym obrocie funkcjonuje pod pojęciem **hackingu**.

Ominięcie[14] zabezpieczenia oznacza działanie, które nie ingeruje bezpośrednio w istniejące zabezpieczenia i nie usuwa ich, lecz polega na ich obejściu.

Art. 267 § 2 k.k. przewiduje karalność czynu, którego skutkiem jest uzyskanie bez uprawnienia dostępu do całości lub części systemu informatycznego.
Definicję systemu informatycznego zawiera art. 7 pkt 2a) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[15]. Zgodnie z powyższym artykułem przez system informatyczny należy rozumieć *zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.*
Do realizacji czynu zabronionego stypizowanego w omawianym przepisie nie jest wymagane przełamanie jakiegokolwiek zabezpieczenia. Nie jest również konieczne, aby sprawca działał w celu uzyskania informacji znajdującej się w zasobach systemu informatycznego lub dostępu do niej.

Jedną z form popełnienia czynu określonego w art. 267 § 2 k.k. jest uzyskanie bez uprawnienia dostępu do systemu informatycznego lub jego części w wyniku wprowadzenia do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem innego użytkownika w celu wykorzystania go jako narzędzie do bezprawnych działań, np. do przeprowadzenia ataków na określone strony internetowe. Takie zachowanie bywa określane mianem **spoofingu**.

Art. 267 § 3 k.k. penalizuje zachowanie polegające na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania informacji, do której sprawca nie jest uprawniony. Przedmiotowy przepis obejmuje czyny stanowiące element przestępczej działalności określanej w potocznym obiegu jako kradzież tożsamości.
Karalne jest już samo założenie lub posłużenie się urządzeniem wymienionym w § 3 wyżej wymienionego przepisu lub oprogramowaniem w celu uzyskania informacji. Do realizacji czynu zabronionego określonego w art. 267 § 3 k.k. nie jest wymagane przełamanie jakichkolwiek zabezpieczeń. Nie jest też konieczne uzyskanie samej informacji, której przechwycenie było celem działań polegających na założeniu lub posłużeniu się wyżej wymienionymi urządzeniami lub oprogramowaniem.
Przez urządzenie podsłuchowe i wizualne należy rozumieć urządzenie służące do rejestracji dźwięku i obrazu, w szczególności takie jak: kamera, aparat cyfrowy, dyktafon.
Za inne urządzenie, o którym mowa w art. 267 § 3 k.k., należy m.in. uznać specjalne techniki polegające na uzyskiwaniu informacji poprzez analizę uderzeń w klawiaturę komputera lub poprzez analizę identyfikatorów i haseł użytkowników.

Oprogramowaniem najczęściej wykorzystywanym do podsłuchu komputerowego jest oprogramowanie szpiegujące (tzw. spyware), które umożliwia przejmowanie treści informacji oraz monitorowanie ruchu w sieci.

[14] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 51.
[15] t.j. Dz.U. z 2002 r., Nr 101, poz. 926 z późn. zm.

Do programów szpiegujących zaliczane są m.in.[16]:

- **keyloggers** (rejestrator klawiatury) – rejestruje wszystkie wpisy użytkownika dokonywane z użyciem klawiatury; użycie tego programu pozwala sprawcy odczytać hasło lub inne dane, które użytkownik komputera wpisał podczas korzystania z usług bankowości elektronicznej,
- **browser hijacker** – umożliwia przejęcie strony internetowej i zmianę jej ustawień powodując np. przekierowanie użytkownika na inne strony,
- **password sniffer** – przechwytuje początkową sekwencję danych każdej sesji, zawierającą identyfikatory i hasła użytkowników danej sieci.

Podkreślić należy, że programy spyware zasadniczo nie rozpowszechniają się same. Do zainfekowania komputera zwykle dochodzi poprzez wprowadzenie użytkownika w błąd lub wykorzystanie luk w oprogramowaniu.

Wprowadzenie do komputera oprogramowania umożliwiającego uzyskiwanie przez osobę nieupoważnioną informacji przekazywanych w sieci komputerowej, np. hasła lub loginu, wypełnia znamiona art. 267 § 3 k.k.

W oparciu o wyżej wymieniony przepis należy m.in. dokonywać kwalifikacji prawnej czynu polegającego na przechwytywaniu danych dotyczących konta bankowego podczas sesji połączeniowych za pomocą urządzenia wymienionego w § 3 lub oprogramowania. Czyn przewidziany w art. 267 § 3 k.k. stanowi formę przestępczej działalności określanej jako **sniffing**.

Sniffing odnosi się do przechwytywania przez niepowołane do tego osoby informacji przesyłanych w lokalnych sieciach, a także sieciach WiFi. W tym celu wykorzystywane są programy komputerowe zwane snifferami, które odbierają i analizują dane z sieci. Działając w powyższy sposób sprawca może uzyskać dane osobowe, którymi np. posłuży się w celu uzyskania korzyści majątkowej kosztem osoby, której dane bezprawnie wykorzystuje. Używając danych osobowych, sprawca może również podszywać się pod swoją ofiarę i podejmować działania na jej szkodę. Śledząc przy użyciu sniffera transakcje finansowe wykonywane za pośrednictwem sieci internet, sprawca może również uzyskać dane dostępowe do konta internetowego, które następnie wykorzysta pozbawiając ofiarę środków zgromadzonych na rachunku bankowym.

Podsumowując powyższe rozważania dotyczące stosowania art. 267 k.k. w odniesieniu do bankowości elektronicznej można najogólniej stwierdzić, że zakresem wyżej wymienionego przepisu objęte są zachowania polegające na nieuprawnionym przejęciu danych w czasie transmisji w środowisku elektronicznym, np. danych z karty płatniczej, czy też danych (login, hasło) służących w bankowości internetowej do identyfikacji użytkownika i uwierzytelniania poleceń, umożliwiających dostęp do środków zgromadzonych na rachunku bankowym.

[16] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 122.

Jako przestępstwo z art. 267 k.k. należy również kwalifikować zachowanie polegające na zakładaniu na bankomatach urządzeń do nielegalnego zbierania informacji z karty płatniczej, będące częścią przestępczej działalności określanej ogólnie mianem **skimmingu**. **Zachowanie sprawcy polega na zakładaniu na powierzchni bankomatu lub w jego pobliżu urządzeń takich jak, np. miniaturowa kamera i czytnik kart, których zadaniem jest odczytanie informacji związanych z kartą płatniczą, tj. numeru PIN oraz skopiowanie danych z paska magnetycznego.** Do realizacji wyżej wymienionego czynu zabronionego wystarczające jest uzyskanie w powyższy sposób informacji związanych z kartą, bez względu na to, jak zostały te informacje dalej wykorzystane, a więc czy sprawca zapoznał się z nimi, czy też je zniszczył uniemożliwiając dalsze ich wykorzystanie, jak też czy skopiowane z paska magnetycznego dane zostały przez sprawcę wykorzystane do podrobienia karty. W przypadku przekazania innej osobie danych skopiowanych z paska magnetycznego karty, zastosowanie znajdzie § 4 omawianego przepisu, penalizujący zachowanie polegające na ujawnieniu innej osobie informacji uzyskanych w którykolwiek ze sposobów określonych w § 1, 2 lub 3 art. 267 k.k.

Art. 268 k.k.
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

Art. 268a k.k.
§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,
podlega karze pozbawienia wolności do lat 3.

Przedmiotem ochrony art. 268 k.k. są: integralność i kompletność zapisu informacji oraz dostępność do istotnej informacji rozumianej jako możliwość swobodnego z niej korzystania przez osoby do tego uprawnione.
Ochroną art. 268a k.k. objęte są: integralność i kompletność zapisu informacji w postaci danych informatycznych, dostępność informacji w postaci danych informatycznych oraz prawidłowość funkcjonowania programów komputerowych.
Przedmiot czynności wykonawczej sprawcy w omawianych przepisach stanowią: zapis istotnej informacji, zapis na informatycznym nośniku danych, zapis informacji w postaci danych informatycznych.
Na podstawie art. 268 k.k. chroniona jest istotna informacja. Istotność informacji będącej przesłanką odpowiedzialności karnej za przestępstwo określone w wyżej wymienionym przepisie jest kategorią ocenną, do której powinny znaleźć zastosowanie kryteria obiektywne. Zasadniczymi elementami branymi pod uwagę przy ocenie istotności informacji winny zatem być: znaczenie

informacji dla podmiotu, którego informacja dotyczy (obiektywnie oceniane), jej treść, waga, przeznaczenie. Przy ocenie powinny być brane również pod uwagę standardy obowiązujące w danej dziedzinie, do której odnosi się informacja. Nie można wykluczyć jednak sytuacji, gdy w konkretnych, uzasadnionych okolicznościami stanu faktycznego przypadkach zostaną uwzględnione również elementy subiektywizujące, np. interes osoby uprawnionej do zapoznania się z informacją.
Szerokie spektrum możliwych odmian czynności wykonawczej w omawianych przepisach obejmuje: niszczenie, uszkadzanie, usuwanie, zmianę zapisu informacji, udaremnianie lub znaczne utrudnianie zapoznania się z informacją; niszczenie, uszkadzanie, usuwanie, zmianę lub utrudnianie dostępu do danych informatycznych, istotne zakłócanie lub uniemożliwienie automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.
Wyżej wymienione czynności są realizowane przede wszystkim przez wprowadzanie do systemów komputerowych specjalnych, w tym złośliwych programów, których celem jest destrukcyjne oddziaływanie na dane informatyczne tych systemów, pracę programów, a także funkcjonowanie całych systemów komputerowych. Te specjalne programy zwane są popularnie wirusami komputerowymi, koniami trojańskimi, bombami logicznymi, robakami komputerowymi.

Wirus komputerowy to samo replikujący się program umieszczany w innym programie (nosicielu), który może w swojej strukturze zawierać zarówno konia trojańskiego, jak i bombę logiczną.
Skutki działania wirusów mogą być bardzo różne i w zasadzie zależą od wyobraźni ich autora. Efekty szkodliwego działania wirusa po zainfekowaniu systemu mogą polegać m.in. na:

- nieupoważnionym kasowaniu danych,
- rozsyłaniu spamu poprzez pocztę elektroniczną,
- dokonywaniu ataków na inne hosty w sieci, w tym serwery,
- kradzieży danych: haseł, numerów kart płatniczych, danych osobowych,
- zatrzymaniu pracy komputera, w tym całkowite wyłączenie wyświetlania grafiki i/lub odgrywania dźwięków,
- utrudnieniu lub uniemożliwieniu pracy użytkownikowi komputera,
- przejęciu przez osobę nieupoważnioną kontroli nad komputerem poprzez sieć.

Bomby logiczne – rodzaj wirusa, który może pozostać w ukryciu przez długi czas. Jego aktywacja następuje w momencie nadejścia określonej daty lub wykonania przez użytkownika określonej czynności.

Robak komputerowy rozpowszechnia się z wykorzystaniem sieci komputerowych i wykorzystuje dane, pliki znajdujące się w zainfekowanych komputerach. W przeciwieństwie do wirusa komputerowego nie niszczy danych i nie przekształca plików, ale może prowadzić do obciążenia programów komputerowych, takich jak np. Firewall, serwer mailowy, powodując znaczne utrudnienia lub uniemożliwienie korzystania z nich. Robaki komputerowe są zwykle rozpowszechniane przy użyciu poczty elektronicznej w celu uzyskania informacji na temat aktywności użytkowników w internecie.

Konie trojańskie (trojany) – to programy z pozoru mogące się wydawać pożyteczne, w rzeczywistości jednak realizują bez wiedzy użytkownika inne funkcje, jak np. przechwytywanie loginów i haseł dostępowych. Uruchamiają się, gdy użytkownik podejmuje pracę z danym programem. Dają atakującemu całkowitą władzę nad komputerem ofiary.

Trojany umożliwiają m.in.:

- pozyskiwanie danych osobowych użytkownika i innych poufnych informacji, jak np. hasła dostępowe i loginy do kont internetowych, informacje o kartach kredytowych,
- pobieranie, modyfikowanie, usuwanie, wysyłanie plików z komputera użytkownika,
- oglądanie ekranu użytkownika,
- wykorzystywanie przestrzeni dyskowej użytkownika,
- zawieszenie komputera.

Art. 286 k.k.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

lub

Art. 287 k.k.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

W odróżnieniu od tradycyjnego oszustwa, którego znamiona określone zostały w art. 286 k.k., art. 287 k.k. (oszustwo komputerowe) penalizuje zachowanie polegające na wpływaniu – bez upoważnienia i w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody – na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianie, usunięciu albo wprowadzeniu nowego zapisu danych informatycznych.

Zasadnicza różnica pomiędzy oszustwem tradycyjnym z art. 286 k.k. a oszustwem komputerowym z art. 287 k.k. polega na tym, że w przypadku oszustwa tradycyjnego działanie sprawcy jest ukierunkowane na osobę, tzn. sprawca wprowadza inną osobę w błąd albo wyzyskuje błąd innej osoby lub niezdolność do należytego pojmowania przedsiębranego działania. Natomiast w przypadku oszustwa komputerowego sprawca wpływa na urządzenia i procesy techniczne związane z automatycznym przetwarzaniem danych wprowadzając niejako „w błąd" maszynę, np. systemy odpowiedzialne za bankowość elektroniczną[17].

To, jaka zostanie zastosowana kwalifikacja prawna będzie zatem zależeć od sposobu działania sprawcy w konkretnym przypadku. Jeżeli działanie sprawcy będzie polegało na oddziaływaniu tylko „na maszynę", to wówczas należy kwalifikować takie zachowanie na podstawie art. 287 k.k. Natomiast jeżeli zachowanie sprawcy będzie dodatkowo zawierało element oddziaływania „na osobę", to wówczas takie zachowanie należałoby kwalifikować z art. 286 k.k.

[17] Ibidem, s. 243.

Wpływanie na urządzenia i procesy techniczne związane z automatycznym przetwarzaniem danych może polegać na wykorzystywaniu w tym celu złośliwego oprogramowania, takiego jak, np.:[18]

- **session hijackiers** – programy umożliwiające ataki polegające na przejęciu sesji legalnego użytkownika i m.in. przejęcie transferu środków pieniężnych,
- **web trojans** – złośliwe oprogramowanie, które umożliwia wyświetlenie strony internetowej zbierającej poufne dane (login, hasło) zamiast oryginalnej strony przeznaczonej do logowania, np. do internetowego konta bankowego,
- **transaction generator** – program atakujący zazwyczaj komputer pośredniczący w procesie przesyłu danych komputerowych, np. komputer odpowiedzialny za przetwarzanie transakcji z wykorzystaniem kart płatniczych.

W zakresie omawianych tu przepisów mieści się również m.in. przestępcze zachowanie zwane **phishingiem**. Mechanizm tego zachowania polega najczęściej na przesyłaniu wiadomości elektronicznych od osób podszywających się pod bank, z prośbą o zalogowanie się na jego stronie internetowej o adresie podanym w tej wiadomości. Link, pod którym należy się zalogować, przypomina oryginalną stronę internetową banku. Sprawcy w różny sposób uzasadniają konieczność zalogowania się na stronie internetowej. Uzasadnieniem może być np. weryfikacja danych karty płatniczej w celu jej przedłużenia, ponownej aktywacji, poprawy bezpieczeństwa transakcji karty w internecie itp. Kliknięcie na link znajdujący się w takiej wiadomości e-mail powoduje „przekierowanie" posiadacza karty płatniczej na stronę internetową przeznaczoną do wprowadzenia danych z karty. W ten sposób przestępcy uzyskują dane dotyczące kart kredytowych, a nawet hasła służące do dokonywania przelewów na specjalnie w tym celu założone konta.
Sprawca może działać w podobny sposób za pomocą telefonu.

Innym sposobem działania przestępcy może być przesłanie posiadaczowi karty płatniczej płyty CD lub innego nośnika informacji. Przesyłka taka zwykle do złudzenia przypomina oryginalną przesyłkę wydawcy karty płatniczej lub innej instytucji. Po włożeniu nośnika do komputera uwalniane są zapisane na niej wirusy lub inne oprogramowanie, które służą do przesyłania przestępcy danych dotyczących karty płatniczej i jej posiadacza.

Formą **phishingu** jest tzw. **pharming**. Polega on na tym, iż po wpisaniu prawidłowego adresu strony internetowej wydawcy karty płatniczej lub innej instytucji, posiadacz karty płatniczej zostaje przekierowany na utworzoną przez przestępcę stronę internetową przypominającą wyglądem oryginalną stronę banku lub innej instytucji.
Wpisywane na tej stronie dane dotyczące karty płatniczej i posiadacza są przechwytywane przez przestępcę.

Zachowanie przestępców może również przybrać postać manipulowania bankomatem polegającego na wyłudzeniu gotówki. Działanie to polega na wpłynięciu na funkcjonowanie bankomatu w taki sposób, aby uzyskać zgromadzoną w nim gotówkę. Przykładem może być wprowadzenie

[18] Ibidem, s. 243-244.

do systemu informatycznego bankomatu wirusa, który umożliwi sprawcy pobranie z bankomatu określonej ilości banknotów.
Innym sposobem działania jest przechwytywanie danych wymienianych pomiędzy bankomatem a centrum autoryzacyjnym, które następnie są modyfikowane albo zastępowane innymi nowymi danymi wprowadzonymi przez sprawcę. W ten sposób mogą być generowane przez sprawcę odpowiedzi z centrum autoryzacyjnego na komputerze podpiętym na linii bankomat – centrum autoryzacyjne, z którego korzysta sprawca umożliwiając wypłacenie gotówki.

Nowym sposobem działania przestępców jest wykorzystywanie przez nich błędów w oprogramowaniu niektórych modeli bezprzewodowych routerów WiFi.
Pozwala to na taką modyfikację konfiguracji routerów, by połączenia z niektórymi polskimi bankami odbywały się poprzez serwery należące do przestępców. Dzięki tym działaniom pozyskują oni identyfikatory i hasła klientów oraz podstawiają zmodyfikowaną stronę banku z komunikatem o wprowadzonej przez niego zmianie formatu rachunku i wynikającej z tego konieczności zatwierdzenia nowego szablonu przelewów zaufanych. Jeśli klient poprawnie zautoryzuje utworzenie takiego szablonu przelewu zaufanego, przestępcy będą w stanie dokonać przelewu środków finansowych klienta na rachunek, nad którym mają kontrolę i w ten sposób dokonać kradzieży[19].

„Nowym sposobem działania przestępców jest wykorzystywanie przez nich błędów w oprogramowaniu niektórych modeli bezprzewodowych routerów WiFi.”

Innym sposobem działania będzie również tzw. oszustwo nigeryjskie (patrz wyżej pkt 1.8.)

Art. 190a. k.k.
§ 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności do lat 3.
§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej.

Czyn penalizowany w art. 190a § 2 k.k. polega na podszywaniu się pod inną osobę, wykorzystaniu jej wizerunku lub danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej. Definicja danych osobowych zawarta jest w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Stosownie do art. 6 ust. 1 tej ustawy, za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

[19] Komunikat Związku Banków Polskich z dnia 6 lutego 2014 r. dostępny pod adresem http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci/komunikat-zagrozenie-dla-klientow-bankowosci-internetowej-korzystajacych-z-routerow-wifi.

Omawiany przepis dotyczy m.in. zachowania polegającego na podszyciu się przez sprawcę pod inną osobę z wykorzystaniem jej danych osobowych podczas zakładania rachunku bankowego, na który następnie przesyłane są pieniądze pochodzące z przestępstw (szerzej patrz pkt 1.7.).

4.1.2 Kierunki pozyskiwania dowodów w postępowaniach w sprawach karnych dotyczących przestępstw w bankowości elektronicznej

Przystępując do analizy problematyki działań wykrywczych i pozyskiwania dowodów popełnienia przestępstw związanych z bankowością elektroniczną, należy wskazać, iż zgodnie z opartym na tradycyjnym rozumieniu śladów kryminalistycznych założeniem, każde zdarzenie zachodzące w otaczającym nas świecie zewnętrznym, w tym każda aktywność człowieka pozostawia jakieś ślady. Przesądza to o skierowaniu poszukiwania śladów, w szczególności na miejscu lub na uczestnikach zdarzenia, jak również na znajdujących się tam przedmiotach, etc. Stwierdzone w ten sposób ślady mogą m.in. stanowić podstawę do wykazania obecności konkretnych osób na miejscu zdarzenia, w tym sprawstwo ściśle określonej osoby/osób.

„Należy stwierdzić, że przestępstwa związane z bankowością elektroniczną stanowią specyficzną kategorię czynów zabronionych opartych na płatnościach bezgotówkowych i elektronicznym przetwarzaniu danych."

W powyższym kontekście należy stwierdzić, że przestępstwa związane z bankowością elektroniczną stanowią specyficzną kategorię czynów zabronionych opartych na płatnościach bezgotówkowych i elektronicznym przetwarzaniu danych.

To specyficzne środowisko bankowości elektronicznej, w którym dochodzi do popełnienia przestępstwa przesądza o charakterze śladów przestępczej aktywności.
W przypadku przestępstw w bankowości elektronicznej ślady w tradycyjnym znaczeniu występują w ograniczonym zakresie, natomiast podstawową rolę odgrywają ślady w elektronicznym zapisie.
Przepisy prawa nie przewidują definicji legalnej dowodu elektronicznego, natomiast dowód ten jest dopuszczalny w procesie karnym.

Dowodem elektronicznym jest informacja przechowywana lub przesyłana w postaci elektronicznej o znaczeniu dowodowym, a więc informacja np. zapisana na nośniku elektronicznym (dysku twardym komputera, w pamięci telefonu), dokument komputerowy (teksty tworzone w Wordzie, zdjęcia), dane cyfrowe (tzw. logi komputerowe) np. ukazujące historię logowania z danego IP komputera na dany serwer.

Z uwagi na specyficzne cechy dowodów elektronicznych, które w porównaniu z tradycyjnymi dowodami stanowią istotne novum wymagające uwzględnienia ich odrębności w procesie dowodzenia oraz zważywszy na fakt, że w praktyce organów ścigania i wymiaru sprawiedliwości dowody elektroniczne będą odgrywały coraz istotniejszą rolę ze względu na rosnącą liczbę przestępstw pozostawiających ślady elektroniczne, rozważania zawarte w tej części publikacji koncentrować się będą głównie na omówieniu cech dowodów elektronicznych oraz związanych z nimi trudnościach dowodowych, a także przedstawieniu problematyki dotyczącej zasad postępowania z dowodami

elektronicznymi na etapie ich pozyskiwania, zabezpieczania, analizy i przechowywania, mających zapewnić możliwość późniejszego ich wykorzystania przed sądem w postępowaniu karnym w celu wykazania popełnienia czynu zabronionego oraz winy sprawcy.
A. Lach[20] wskazuje m.in. na następujące cechy szczególne dowodów elektronicznych: łatwość modyfikacji, przechowywania, powielania; poszlakowy charakter – pozwala identyfikować wiedzę sprawcy, a nie jego tożsamość; podpis pod dokumentem elektronicznym lub dane nadawcy w nagłówku nie identyfikują autora; dane identyfikujące zakończenie sieci nie wskazują osoby użytkującej urządzenie w danym czasie; łatwo go usunąć lub przenieść w inne miejsce, trudno natomiast zniszczyć go definitywnie, z tego powodu ważne jest właściwe jego zabezpieczenie i przechowywanie.

Specyfika przestępstw w bankowości elektronicznej, a w szczególności bankowości internetowej polega na oddzieleniu miejsca pobytu (działania) sprawcy od miejsca wystąpienia skutku jego przestępczego działania. Z reguły bowiem miejsca te, pod względem położenia geograficznego, mają różne lokalizacje i nierzadko bywa, że są one znacznie oddalone od siebie.

Oczywiście w praktyce możliwe są o wiele bardziej skomplikowane stany faktyczne związane z ustaleniem miejsca przestępczej aktywności, która może obejmować terytorium kilku państw. Za przykład można wskazać sytuację, gdy na terytorium jednego państwa dochodzi do przestępstwa polegającego na bezprawnym skopiowaniu podczas korzystania z bankomatu zawartości paska magnetycznego karty płatniczej oraz uzyskaniu numeru PIN karty za pomocą urządzeń, takich jak np. czytnik kart i miniaturowa kamera (skimming karty płatniczej).
Uzyskane w ten sposób dane przesyłane są za pośrednictwem sieci internet do odbiorcy znajdującego się na terytorium innego państwa. Dochodzi tam wówczas do popełnienia przestępstwa podrobienia karty płatniczej. Polega ono na nagraniu skopiowanej zawartości paska magnetycznego oryginalnej karty na pasek innej, imitującej oryginalną. Następstwem opisanych działań jest dokonanie przestępstwa na terytorium innego państwa.

Do realizacji omawianych przestępstw nie jest wymagana fizyczna obecność sprawcy w miejscu jego popełnienia.

Możliwe jest bowiem zdalne uruchomienie programu przez sprawcę, który zamierza np. wprowadzić do systemów innych użytkowników zainfekowany program w celu przejęcia danych umożliwiających dostęp do kont klientów banku, takich jak hasła czy też kody autoryzujące.
W takim więc przypadku nie dojdzie do pozostawienia przez sprawcę klasycznych śladów w miejscu popełnienia przestępstwa. Zwykle też nie dojdzie w tym miejscu do osobistej interakcji sprawcy i pokrzywdzonego, jak to bywa, co do zasady, w przypadku tradycyjnych przestępstw.
Problem zyskuje w szczególności na znaczeniu w przypadku przestępstw popełnianych za pośrednictwem sieci internet, która ma ogólnoświatowy zasięg i w zasadzie daje nieograniczoną terytorialnie możliwość popełniania przestępstw poprzez działania na odległość, np. zdalne uruchomienie programu, który następnie przystępuje w komputerze innego użytkownika do realizacji zaplanowanego przestępstwa.

[20] G. Nauka, VI edycja seminarium z cyklu „Prawnicza informatyka korporacyjna" nt. „Dowody elektroniczne w postępowaniu karnym" (Warszawa, 12.08.2008 r.), Prokuratura i Prawo 7-8, 2008, s. 251-252.

Dostęp do sieci internet generuje zjawisko tzw. przestępczości transgranicznej, która stwarza dodatkowe utrudnienia dla prowadzenia działań wykrywczych, wynikające z odrębnej jurysdykcji państw, na terytorium których dochodzi do przestępczych działań, często od siebie bardzo odległych, o odmiennej kulturze prawnej, wymagające nawiązania wzajemnej współpracy pomiędzy organami ścigania tych państw, co znacznie wydłuża czas podjęcia stosownych działań, a to z kolei potęguje ryzyko usunięcia w tym czasie danych w formie elektronicznej, co należy do stosunkowo łatwych czynności.

Należy dodać, że problem współpracy transgranicznej pomiędzy uprawnionymi organami poszczególnych państw, obejmującej m.in. ustanowienie szczególnych procedur dotyczących wykrywania i ścigania sprawców przestępstw, w tym gromadzenia dowodów popełnionych przez nich czynów zabronionych, wymianę informacji pomiędzy punktami kontaktowymi, etc., został rozwiązany częściowo – ze względu na ograniczony zakres terytorialny stosowania – w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.

Sprawca popełniający przestępstwo za pomocą internetu nie pozostawia tradycyjnych śladów identyfikujących, takich jak np. pismo ręczne, ślady biologiczne, daktyloskopijne, co powoduje, że indywidualizm sprawcy ulega zatarciu.
Te wszystkie wskazane wcześniej przyczyny utrudniają wykrycie przestępstw w bankowości elektronicznej oraz ich sprawców, a także proces dowodzenia oparty na śladach elektronicznych wykazujących relatywnie niewielką przydatność, w szczególności w zakresie udowodnienia winy sprawcy.

Specyfika logu cyfrowego jako dowodu elektronicznego

Należy zauważyć, że korzystanie z internetu nie oznacza jednakże całkowitej anonimowości, przynajmniej jeśli chodzi o identyfikację urządzenia, np. komputera, którym sprawca posłużył się dokonując przestępstwa poprzez internet czy też miejsca, w którym się znajdował w czasie dokonywania przestępstwa.
Każde bowiem urządzenie podpięte do sieci posiada unikatowy w danej chwili adres zwany numerem IP (Internet Protocol). Adres IP nie jest bowiem przydzielany na stałe użytkownikowi, lecz jest przypisywany za każdym razem podczas łączenia się z siecią internetową na czas bytności danej osoby w sieci. Ta chwilowa unikatowość adresu IP przydzielonego podczas konkretnego łączenia się z internetem w powiązaniu z dokładnym określeniem czasu (daty i godziny korzystania z tego IP) pozwala jednoznacznie zidentyfikować urządzenie (np. komputer) w sieci internet.
W ten sposób poprzez ustalenie lokalizacji komputera, możliwa jest identyfikacja miejsca, z którego działano. Na tej podstawie możliwe jest również uzyskanie informacji o konkretnych stronach internetowych, które były odwiedzane w określonym czasie, ustalenie treści przesyłanych plików.

Dane pozwalające uzyskać informacje, jaki komputer korzystał z określonego IP w określonym czasie gromadzone są na logach cyfrowych.

Logi dotyczące usług internetowych zawierają informacje odnoszące się do tego, kiedy i kto, tj. jaki adres IP korzystał z danego serwisu.

Aby logi cyfrowe mogły być wykorzystane jako dowody w postępowaniu karnym, muszą spełnić warunki pozwalające uznać je za integralne i niepodważalne dowody.
Dokonując oceny wartości dowodowej logów cyfrowych należy w szczególności zwrócić uwagę na podatność logów na modyfikowanie i preparowanie, wynikającą z faktu przechowywania logów na nośnikach wielokrotnego zapisu, co daje praktycznie nieograniczoną możliwość ingerowania w ich treść. Niezbędne jest również ustalenie, czy dostęp do zawartych w nich danych został zabezpieczony w sposób uniemożliwiający dokonanie zmian jakichkolwiek zapisów w logach cyfrowych. Dla oceny wartości dowodu z logów cyfrowych, istotne znaczenie ma także zbadanie programu komputerowego służącego do rejestracji logów pod kątem sprawdzenia, czy funkcjonuje prawidłowo. W przypadku ustalenia, że program zawiera błędy powodujące nieprawidłowy zapis logów, dowodu takiego nie będzie można wykorzystać w postępowaniu sądowym.

„W oparciu o informacje zawarte w logach cyfrowych można również doprowadzić do ujęcia osób, które włamały się do systemu."

Należy również pamiętać o poszlakowym charakterze wyżej wymienionego dowodu oraz o tym, że nie w każdym przypadku można automatycznie łączyć adres IP komputera z jego użytkownikiem i w konsekwencji na tej podstawie przypisywać mu sprawstwo.

Log cyfrowy nie może być wykorzystany jako dowód, jeśli identyfikuje adres IP komputera, którym posługuje się sprawca do dokonywania przestępstw w sieci wykorzystując zainstalowane na komputerze innego użytkownika złośliwe oprogramowanie umożliwiające przejęcie kontroli nad zainfekowanym komputerem, o czym zwykle nie ma wiedzy użytkownik komputera, pod którego podszywa się prawdziwy sprawca dopuszczający się przestępczych zachowań na „konto" nieświadomego tych działań użytkownika.

W konsekwencji może to skutkować skierowaniem przeciwko niemu fałszywych podejrzeń co do sprawstwa popełnionych w powyższy sposób przestępstw.
Organy ścigania powinny w każdym przypadku przebadać komputer, którego adres IP zawarty był w logach cyfrowych pochodzących z komputera, gdzie nastąpiło włamanie, pod kątem sprawdzenia czy powyżej opisana sytuacja podszywania się pod innego użytkownika z użyciem złośliwego oprogramowania umożliwiającego przejęcie kontroli nad zainfekowanym komputerem nie zachodzi w konkretnej sprawie prowadzonej przez te organy. W przypadku stwierdzenia obecności wyżej wymienionego oprogramowania umożliwiającego przejęcie kontroli nad zaatakowanym komputerem, dowód z logów cyfrowych będzie nieprzydatny z punktu widzenia możliwości wykorzystania go w postępowaniu przed organami wymiaru sprawiedliwości[21].
Podobnie bezużyteczny dla toczącego się postępowania będzie dowód z logów cyfrowych w przypadku, gdy adres IP wskaże na korzystanie z komputera znajdującego się w kawiarence internetowej, gdzie każdy ma zapewniony swobodny dostęp do komputera bez konieczności rejestracji, co uniemożliwia identyfikację sprawcy.

Z wyłączeniem zatem sytuacji, takich jak: maskowanie działań, posługiwanie się komputerem innej osoby bez jej wiedzy, korzystanie z kawiarenki internetowej, gdzie można korzystać z kompu-

[21] M. Kliś, A. Stella-Sawicki, *Identyfikacja użytkownika komputera na podstawie logów cyfrowych*, Prokuratura i Prawo 7-8, 2001, s. 51-62.

terów bez konieczności jakiejkolwiek rejestracji, co praktycznie uniemożliwia identyfikację sprawcy, czy też podszywanie się pod innego użytkownika sieci z użyciem złośliwego oprogramowania, kiedy dopuszczenie logów cyfrowych jako dowodów w postępowaniu karnym nie będzie możliwe, w pozostałych przypadkach, pod warunkiem zabezpieczenia dowodu z logu cyfrowego w prawidłowy sposób, log cyfrowy identyfikujący adres IP komputera będzie mógł posłużyć jako dowód poszlakowy wskazujący pośrednio na sprawstwo użytkownika zidentyfikowanego adresu IP.

Poszlaką jest fakt, z którego pośrednio może wynikać sprawstwo określonej osoby. W powiązaniu z innymi dowodami i poszlakami zwiększa się prawdopodobieństwo wykazania, kto zasiadał za klawiaturą w badanym okresie. Inne dowody to np. ustalenie na podstawie osobowych źródeł dowodowych, że w określonym czasie z komputera mógł korzystać tylko jego użytkownik albo że poza użytkownikiem nikt inny nie ma dostępu do komputera. Poszlaką może być również brak alibi użytkownika komputera, z którego nastąpił atak na okoliczność, że w czasie, w którym doszło do przestępczej aktywności w sieci użytkownik znajdował się w innym miejscu niż przy klawiaturze komputera, którego adres IP został zidentyfikowany przez log cyfrowy, jako adres IP komputera, z którego nastąpił przestępczy atak.

W tym kontekście należy wskazać, że modus operandi sprawcy przestępstwa w bankowości elektronicznej polegającego np. na podrobieniu internetowej strony bankowej i przekierowywaniu przelewów lub wpłat na inne konta, czy też przechwytywaniu danych dotyczących konta bankowego podczas sesji połączeniowych, obejmujący takie właściwości jak: ogromna wiedza, szczególne kwalifikacje w zakresie informatyki, znajomość oprogramowania, a w szczególności jego słabych stron, umożliwiająca wykorzystanie luk i błędów, specyficzna motywacja sprawcy i pobudki, jakimi się kieruje popełniając przestępstwo, może stanowić istotną podstawę działań wykrywczych pozwalającą wytypować ścisły krąg możliwych sprawców. Modus operandi ma zasadniczo głównie charakter poszlakowy pośrednio wskazujący na sprawcę.

Podkreślić należy, że wspomniane wyżej specyficzne cechy dowodów elektronicznych determinują sposób prowadzenia procesu dowodowego.

W pierwszej kolejności istotne jest zapewnienie udziału w czynnościach związanych z poszukiwaniem, zabezpieczaniem i utrwalaniem dowodów elektronicznych osób (ekspertów), które posiadają specjalistyczną wiedzę w zakresie działania sprzętu i systemu komputerowego oraz techniki informatycznej. Ważne jest, aby przystępując do poszukiwania materiału dowodowego, określony był plan działania pozwalający w szczególności uzyskać odpowiedzi na następujące pytania: czego szukamy? (jakich śladów), gdzie?, po co? (jakie okoliczności będzie można wykazać w oparciu o uzyskane dane).

Powyższe działania powinny być podjęte bez zbędnej zwłoki, z uwagi na fakt, że dowody elektroniczne w każdej chwili mogą zostać usunięte z komputera.

„Programy przestępcze często mają wbudowaną procedurę autodestrukcji, która uruchamia się automatycznie po wykonaniu określonego zadania."

Ponadto programy przestępcze często mają wbudowaną procedurę autodestrukcji, która uruchamia się automatycznie po wykonaniu określonego zadania.

Należy jednakże dodać, że zaletą dowodów elektronicznych jest to, że trudno zniszczyć je definitywnie w taki sposób, aby nie pozostał jakikolwiek ślad w elektronicznym

nośniku informacji. Możliwe jest ich odtworzenie przy użyciu dedykowanych w tym celu programów komputerowych, jak np. EasyRecovery, który pozwala odzyskać utracone lub skasowane dane, pliki, foldery. Skasowanie danych przy użyciu komendy „usuń" nie oznacza ich natychmiastowego zniszczenia, a jedynie utratę ścieżki dostępu.

Kolejną bardzo istotną kwestią jest zabezpieczanie, utrwalanie i przechowywanie dowodów elektronicznych. Od tego bowiem, jakie zasady znajdą zastosowanie, jakie techniki i metody zostaną użyte podczas dokonywania powyższych czynności, zależy dalszy los dowodów, a dokładnie możliwość ich późniejszego wykorzystania na etapie czynności dowodowych w postępowaniu sądowym, jako pełnowartościowych dowodów przestępstwa nadających się do przypisania na ich podstawie winy sprawcy bez obawy, że drugiej stronie postępowania uda się skutecznie podważyć ich wiarygodność. Świadomość odpowiedzialności, jaka wiąże się z prawidłowym postępowaniem z ujawnionymi dowodami elektronicznymi, powinna znaleźć odzwierciedlenie w praktyce organów dokonujących zabezpieczenia tego rodzaju dowodów oraz w stosownych procedurach określających zasady gromadzenia, zabezpieczania i przechowywania materiału dowodowego w postaci elektronicznej, mających zapewnić ich wykorzystanie w postępowaniu sądowym jako w pełni wiarygodne, niepodważalne i integralne dowody popełnienia przestępstwa pozwalające przypisać winę sprawcy.
Zmiany do ustawy z dnia 6 czerwca 1997 r., Kodeks postępowania karnego[22], dalej k.p.k. wynikające m.in. z uwzględnienia potrzeb, jakie wiążą się ze wzrastającą rolą dowodów elektronicznych w postępowaniu karnym zostały zapoczątkowane ustawą z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych[23].

Na mocy powyższej regulacji został wprowadzony m.in. art. 236a k.p.k., który zgodnie z jego aktualnym brzmieniem, przewiduje odpowiednie stosowanie przepisów działu V k.p.k. dotyczących zatrzymania rzeczy i przeszukania do *dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną.* W uzasadnieniu projektu wyżej wymienionej nowelizacji w zakresie dotyczącym dodanego art. 236a k.p.k. wskazano, że *świadectwem czasu jest propozycja, aby przepisy o zatrzymaniu rzeczy i przeszukaniu stosować odpowiednio do dysponenta i użytkownika systemu informatycznego w zakresie danych przechowywanych w tym systemie lub nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji już przesłanej pocztą elektroniczną (art. 236a). Projekt ustawowy w tym miejscu oznacza implementację do polskiego prawa konwencji międzynarodowych, których Polska jest stroną.*

[22] Dz.U. Nr 89, poz. 555 z późn. zm.
[23] Dz.U. z 2003 r., Nr 17, poz. 155.

Jak to zostało wcześniej wskazane, **zapewnienie niepodważalnej autentyczności i integralności dowodów elektronicznych** i w konsekwencji dopuszczalności ich wykorzystania w postępowaniu przed organami wymiaru sprawiedliwości, **uzależnione jest od sposobu postępowania z dowodami elektronicznymi na etapie ich pozyskiwania, gromadzenia, zabezpieczania i przechowywania.**
W praktyce organów procesowych oraz w informatyce śledczej stosuje się zasady, w tym metody i techniki postępowania z materiałem dowodowym na etapie jego pozyskiwania, gromadzenia, zabezpieczania i przechowywania, wśród których szczególnie należy zwrócić uwagę na następujące:

- wykonanie kopii nośnika informacji w celu przeprowadzenia na nim szczegółowej analizy danych,
- zabezpieczenie pozyskanych dowodów elektronicznych programem śledczym w celu wykazania w postępowaniu sądowym, że dowody te zostały dostarczone do sądu w niezmienionej i kompletnej formie, a więc takiej w jakiej zostały odnalezione i włączone do materiału dowodowego,
- uwierzytelnienie danych sumą kontrolną,
- dane powinny być dodatkowo dokumentowane fotograficznie ze sporządzeniem pełnego opisu drogi materiału dowodowego z podaniem daty, godziny, osoby, która odpowiadała w konkretnym czasie za dowody oraz miejsca ich magazynowania[24] w celu wykazania, że dowody, które zostały przekazane sądowi dotarły w formie niezmienionej i kompletnej, a więc, że są wiarygodne,
- korzystanie z dowodu w postaci opinii biegłego ze specjalnością w zakresie technik informatycznych, w szczególności do analizy zabezpieczonych danych,
- udział specjalistów w czynnościach organów ścigania związanych z procesem gromadzenia materiału dowodowego na każdym jego etapie, a w szczególności przy zabezpieczaniu śladów elektronicznych podczas czynności zatrzymania danych i przeszukania, w tym m.in. uczestniczenie w przeszukaniu zasobów systemu, kopiowaniu danych,
- dowody powinny posiadać następujące cechy: być legalne, autentyczne, kompletne, dokładne, przekonujące,
- procedury zabezpieczania materiału dowodowego powinny zapewnić dowodom ochronę przed uszkodzeniem, zniszczeniem lub jakąkolwiek inną ingerencją wymierzoną przeciwko ich nienaruszalności i integralności, której skutkiem byłaby możliwość kwestionowania ich wiarygodności,
- analizie podlegają wszelkie dane zgromadzone na komputerowym nośniku informacji, w tym również dane ukryte, skasowane, kopie plików wraz z logami i rejestrami,
- czynności związane z gromadzeniem danych elektronicznych nie mogą naruszać przepisów o tajemnicy ustawowo chronionej, np. tajemnicy bankowej,
- wykorzystanie eksperymentu kryminalistycznego w celu odtworzenia przebiegu zdarzenia realizującego znamiona przestępstwa w elektronicznym obrocie bankowym.

Podsumowując należy stwierdzić, że dopuszczone przez sąd jako materiał dowodowy będą mogły być jedynie te dane, które zostały przygotowane w sposób zapewniający ich integralność i niepodważalną autentyczność, umożliwiając ich wykorzystanie w toku postępowania przed sądem jako pełnowartościowe dowody, których prawdziwość trudno jest zakwestionować.

[24] G. Nauka, VI edycja seminarium z cyklu „Prawnicza informatyka korporacyjna", op. cit., s. 254.

Komisja Nadzoru Finansowego
Pl. Powstańców Warszawy 1
Skr. poczt. nr 419, 00-950 Warszawa 1
Tel. (+48) 22 262 50 00
Fax (+48) 22 262 51 11
knf@knf.gov.pl
www.knf.gov.pl

ISBN 978-83-63380-63-2