dr Wojciech Kasprzak, mgr Agata Opalska

ZAGROŻENIA CYFROWE PRZY PŁATNOŚCIACH ELEKTRONICZNYCH

Według Gooda od momentu wynalezienia elektryczności w 1873 r. do chwili jej masowej adaptacji na całym świecie minęło 46 lat. Telefonom zajęło to 35 lat, radiu 25 lat, komputerom osobistym 16 lat, a Internetowi zaś tylko 6 lat[1]. Rozwój Internetu pociągnął za sobą rozwój cyberprzestępczości, przez którą rozumie się wszelkie stojące w sprzeczności z prawem działania, których celem jest wyrządzenie szkody z wykorzystaniem cyberprzestrzeni i urządzeń cyfrowych[2]. Do tej kategorii przestępstw zalicza się przestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanych informacji, jak np. sabotaż informatyczny, ingerencja w dane i system oraz haking[3]. Ściganie tego typu przestępstw jest możliwe dzięki przepisom zawartym w rozdziale XXXIII Kodeksu karnego. Zgodnie z ogólnymi zasadami odpowiedzialności karnej na gruncie prawa polskiego przestępstwa komputerowe stypizowane w przepisach Kodeksu karnego mogą być popełniane jedynie umyślne, a zatem wówczas kiedy sprawca ma zamiar ich popełnienia, co oznacza, że chce je popełnić albo przewidując możliwość ich popełnienia godzi się na to (art. 9 § 1 k.k.)[4].

W dzisiejszych czasach obywatel dysponuje całą gamą usług pozwalających realizować mu określone czynności za pośrednictwem sieci Internetowej. Dynamiczny rozwój nowych technologii cyfrowych umożliwia usługodawcom przenoszenie znacznej części swojej działalności do przestrzeni wirtualnej[5]. Obrazem takich zmian jest dzisiejszy wygląd Internetu oraz zawartość jaką możemy tam znaleźć. Począwszy od tradycyjnych stron zawierających przydatne informację, kończąc na tysiącach sklepów i ogłoszeń o usługach. Nowe możliwości handlowe wymagały stworzenia nowoczesnego i sprawnie działającego sytemu, opierającego się na płatnościach elektronicznych, wykorzystujących w pełni potencjał jaki daje cyberprzestrzeń. Wprowadzone zostały zatem możliwości tzw. płatności online z wykorzystaniem środków zgromadzonych na koncie bankowym, do których zalicza się m.in.: przelewy internetowe, karta płatnicza, płatność zbliżeniowa, wypłaty bankomatowe itp. Odmiennie traktowane jest pojawienie się nowych odpowiedników waluty cyfrowej, przejawiające się zastosowaniem technologii kryptograficznej oraz dokonywaniem płatności monetami wirtualnymi BitCoin. Duża popularyzacja elektronicznych metod płatniczych spowodowała wykształcenie się nowych form przestępstw na tle cyfrowym. W dzisiejszych czasach łatwiej jest paść ofiarą przestępstwa kradzieży, polegającego na wyczyszczeniu środków z karty kredytowej niż zostać okradzionym przez kieszonkowca. Warto również wspomnieć, że w momencie wprowadzania płatności metodą karty magnetycznej, przeciwni temu zabiegowi byli sami przedsiębiorcy i sprzedawcy. Obawy te wynikały z braku materialnego potwierdzenia dokonania transakcji wymiany towaru na pieniądze. Bowiem zamiast posiadania rzeczywistych pieniędzy sprzedawca miał otrzymać jedynie potwierdzenie dokonania bezpośredniego przelewu z konta bankowego należącego do klienta. Zaproponowany system nie stwarzał jednak gwarancji przeprowadzenia transakcji. W odpowiedzi na wątpliwości sektora handlowego banki zgodziły się na udzielenie owego potwierdzenia, które polegało na ubezpieczeniu sprzedawcy od poniesienia ewentualnych strat wynikających z oszustwa nieuczciwych konsumentów. Gdy pieniądze nie zostały przelane na konto sklepowe wówczas bank pokrywał całość długu. Dopiero wprowadzenie takiej gwarancji pozwoliło sforsować barierę niepewności wokół nowej metody płatności.

Nowoczesne technologie pozwalają dziś na dużo więcej niż prosta płatność kartą kredytową. Użycie urządzeń mobilnych, np. smartfona w autoryzacji transakcji technologią zbliżeniową, wykorzystuje w rzeczywistości programy pozwalające na korzystanie z konta bankowego bezpośrednio z telefonu. Umożliwia to, np. opłacenie podatków bez konieczności odwiedzenia placówki banku, poczty itp. Żądanie wykonania wybranej opcji bankowej może zostać wysłane z każdego miejsca na ziemi, w którym jest zasięg bezprzewodowej sieci Internetowej. Nowe zaproponowane udogodnienia w obsłudze kont bankowych zostały bardzo ciepło przyjęte przez społeczeństwo, bowiem wizja ułatwienia sobie życia i wyeliminowanie konieczności stania w kolejkach w celu opłacenia rachunku, była na tyle efektywna, że sektor bankowy rocznie osiąga miliardowe zyski z działalności w cyberprzestrzeni. Warto również wspomnieć, że wszystkie dodatkowe usługi mobilne świadczone przez banki wymagają minimalnych opłat jedynie przy ich uruchomieniu. Korzystanie z nich w późniejszym okresie pozostaje bezpłatne i dotyczy to wszelkich czynności wykonywanych z nową usługą. Miesięczna opłata pobierana jest w wysokości 1-2zł, co powoduje, iż takie rozwiązanie

[1] Podaję za: Sh. Heffernan, *Nowoczesna bankowość*, Warszawa 2007, s. 113.
[2] J. Kasprzak, B. Młodziejowski, W. Kasprzak, *Kryminalistyka. Zarys systemu*, Warszawa 2015, s. 48.
[3] J. Czapska, *Jak skutecznie zapewniać bezpieczeństwo? Współczesne wyzwania*, [w:] J. Czapska, A. Okrasa (red.), *Bezpieczeństwo - policja – kryminalistyka. W poszukiwaniu wiedzy przydatnej w praktyce*, Kraków 2015, s. 9.
[4] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, s. 209.
[5] J. Plis: "*Komunikacja w cyberświecie*", red. S. Bębas, J. Plis, J. Bednarek, Radom 2012, s. 357

staje się zdecydowanie korzystniejsze aniżeli dokonanie opłaty bezpośrednio w placówce banku, która średnio wynosi 5-8zł. Każda transakcja przeprowadzana w Internecie jest odpowiednio zabezpieczana przez systemy bezpieczeństwa usługodawcy i certyfikaty bezpieczeństwa zawarte w stronach internetowych odpowiednich instytucji, np. banków. Nie gwarantuje to jednak całkowitego zabezpieczenia płatności dokonywanej cyfrowo. Wszystkie technologie posiadają dziury systemowe i luki, które można wykorzystać w celu dokonania kradzieży pieniędzy wirtualnych. Służą do tego programy komputerowe tworzone przez hakerów oraz techniki wykradania informacji bezpośrednio od użytkownika sieci, czego przykładem może być metoda phishing[6]. Nierzadko zdarza się, iż użytkownicy otrzymują na skrzynce mailowej wiadomości niewiadomego pochodzenia, zawierające podejrzane załączniki. Istnieje duże prawdopodobieństwo, że tego rodzaju e-maile zawierają pewien typ złośliwego oprogramowania, służącego do kradzieży danych pochodzących z komputera. Przykładem może być program keylogger, monitorujący sekwencje wciskanych klawiszy na klawiaturze, a następnie wyodrębnienie z nich loginów i haseł do usług internetowych. W pozostałych przypadkach podejrzane e-maile mogą być próbą wyłudzenia danych umożliwiających dokonanie kradzieży.

Przestępstwo kradzieży penalizuje treść art. 279 k.k., który wskazuje na kwalifikowany typ kradzieży w postaci kradzieży z włamaniem. Czyn ten obejmuje znamiona kradzieży zwykłej, a dodatkowo okoliczność kwalifikującą w postaci sposobu działania, polegającego na włamaniu. Wobec powyższego chroni te same dobra co zwykła kradzież[7]. W odróżnieniu od niej jest natomiast przestępstwem bez względu na wartość rzeczy (art. 130 § 2 KW)[8]. Włamaniem jest nie tylko działanie, którego istotą jest pokonanie zabezpieczenia, jak np. wyłamanie drzwi, czy przecięcie kłódki, ale też pokonanie przeszkody w inny sposób, jak np. otwarcie zamka podrobionym kluczem, zerwanie plomby, czy otwarcie kasy przy wykorzystaniu skradzionego hasła szyfrowego[9]. Włamaniem należałoby również określić wszelkie metody dostania się do zabezpieczonego obszaru cyfrowego. Ustawodawca definiuje przestrzeń zamkniętą jako obszar zabezpieczony przed nieautoryzowanym dostępem, nie tłumacząc czym dokładnie jest owa przestrzeń. W takim wypadku można wysunąć twierdzenie, iż włamanie do zabezpieczonej hasłem i loginem przestrzeni cyfrowej wyczerpuje wszelkie znamiona potrzebne do zakwalifikowania takiego czynu przestępczego jako kradzieży z włamaniem. Aby doszło do włamania, rzecz stanowiąca przedmiot wykonawczy kradzieży musi znajdować się w zamkniętym pomieszczeniu lub jego odpowiedniku, np. poczta mailowa. Sprawca włamuje się do pomieszczenia wskutek likwidacji przeszkody materialnej lub wirtualnej w przypadku płaszczyzny cyfrowej, stanowiącej część konstrukcji pomieszczenia lub systemu[10]. Sposób pokonania bariery jest bez znaczenia. Włamanie nie wymaga jej zniszczenia, uszkodzenia, wykorzystania siły fizycznej, czy użycia jakiegokolwiek narzędzia[11]. Przestępstwa kradzieży z włamaniem charakteryzują się znaczącą rozpiętością z perspektywy społecznej szkodliwości czynów, poczynając od bardzo poważnych do czynów drobnych, objętych pojęciem wypadków mniejszej wagi[12]. Podobnie jak ma to miejsce w przypadku kradzieży z włamaniem w świecie realnym, również przestępcy komputerowi łamią różnego rodzaju zabezpieczenia sieci i systemów komputerowych, ściągają tajne informacje, niekiedy celem ich dalszej odsprzedaży lub włamują się do systemów bankowych, dokonując tam niewielkich kradzieży. Złodzieje komputerowi działają na zlecenie, mogą przejmować cudzą korespondencję, podsłuchiwać, przejmować pliki, włamywać się do określonych komputerów, zarażać wirusami firmowe sieci na zlecenie konkurencji albo też dokonywać na własny bądź cudzy rachunek nielegalnych przelewów[13]. Dostęp do zdecydowanej większości systemów komputerowych i serwisów sieciowych, opiera się na tradycyjnych hasłach w postaci ciągów alfanumerycznych. Istotnym jest, że bezpieczeństwo tych metod uwierzytelniania zależy w dużym stopniu od użytkowników, tj. ich możliwości pamięciowych, rozumienia problemu, poczucia odpowiedzialności i motywacji. Przeprowadzane informacje dowodzą, że awarie systemów wiążą się w dużym stopniu z możliwością wyboru haseł przez użytkowników oraz sytuacjami, w których hasła są im przypisywane. Zgodnie z powszechną, aczkolwiek nieformalną zasadą hasła łatwe do zapamiętania są tym samym łatwe do złamania, z kolei zaś hasła odpowiadające wymogom bezpieczeństwa z reguły przekraczają ludzkie chęci i

[6] Technika hakerska phishing (wędka z przynętą) polega na uzyskaniu danych i dostępie do komputera ofiary, przez wysłanie maila o tematyce będącej w kręgach zainteresowania ofiary (np użytkownik interesuje się bronią, zatem na podstawie analizy i śledzenia w Internecie haker uzyskuje informację gdzie ofiara bywa w sieci i jakich informacji szuka. Na bazie uzyskanych informacji tworzone są maile zawierające poszukiwane przez ofiarę dane i zainfekowany złośliwym oprogramowaniem). Technika spear-phishing wykorzystywane jest w celu ataku na określoną osobę, a nie grupę osób. Najczęściej z tej drugiej metody korzysta się w celu ataku na ofiarę będącą w posiadaniu kluczowych informacji lub danych np firmy lub bankowych.

[7] A. Grześkowiak (red.), *Prawo karne*, wyd. 2 popr. i uzup., Warszawa 2009, s. 370.

[8] Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (Dz.U. 2015 poz. 1094).

[9] L. Gardocki, *Prawo karne*, wyd. XIV zm., Warszawa 2008, s. 319-320.; Uchwała SN z dnia 25.06.1980 r., VII KZP 48/78, OSNKW 1980, Nr 8, poz. 65.

[10] Wyrok SN z dnia 18.12.2002r., III KKN 423/00, Prok. I Pr. 2003, Nr 8, poz. 16.

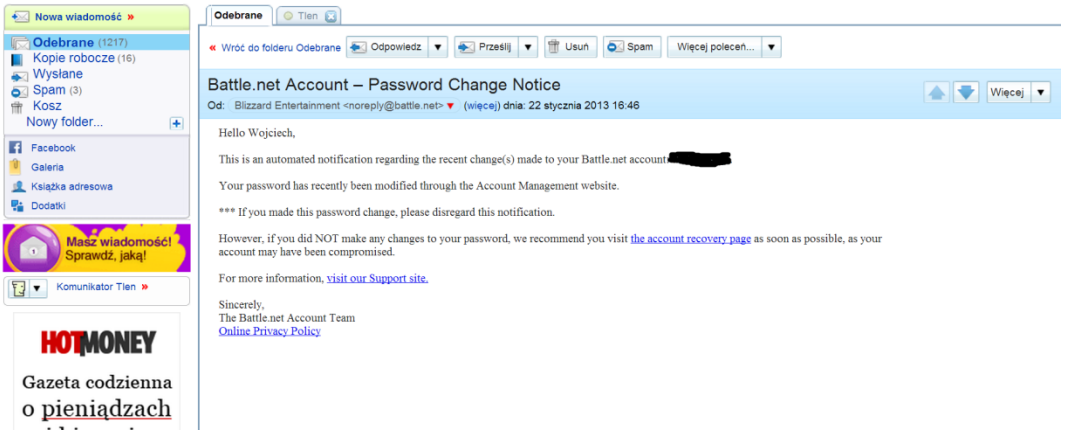
[11] A. Grześkowiak, *op.cit*., s. 370.

[12] A. Marek, *Prawo karne w pytaniach i odpowiedziach*, wyd. 8 zm. i zaktual., Toruń 2007, s. 311.

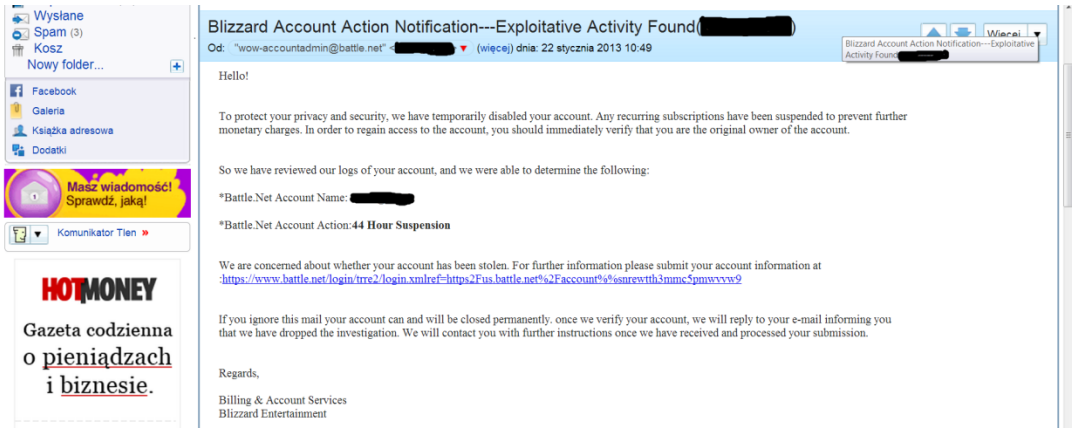
[13] B. Hołyst, *Zagrożenia ładu społecznego*, tom I, Warszawa 2013, s. 83.

możliwości ich zapamiętania. Słabość tradycyjnych metod powoduje, że uwierzytelnianie z użyciem haseł nie gwarantuje należytego poziomu bezpieczeństwa[14].

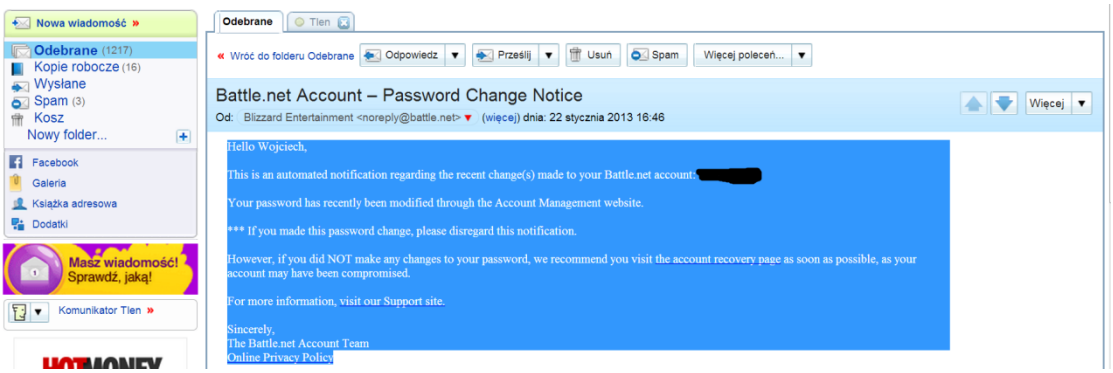
Można wyróżnić kilka metod i technik, jakimi posługują się przestępcy by dokonać kradzieży pieniędzy w cyberprzestrzeni. Pierwszą metodą jest uzyskanie dostępu do danych chronionych i newralgicznych, których udostępnienie osobom postronnym może skutkować nieautoryzowanym dostępem np. do konta bankowego, karty kredytowej lub wirtualnego portfela (serwis paypal). Głównym czynnikiem odpowiedzialnym za upublicznienie danych będzie w tym przypadku czynnik ludzki oraz niezachowanie odpowiedniej ostrożności. Dane zostaną pozyskane bezpośrednio od ofiary na podstawie przeprowadzonej rozmowy lub pewnych technik wyłudzających informacje. Mogą to być prymitywne pytania z prośbą o udostępnienie takich informacji przez komunikator internetowy lub na forum publicznym w sieci. Innym razem ofiara może otrzymać e-mail o niepokojącej treści, będący próbą oszustwa.



Ryc. 1 Przykład wiadomości potwierdzającej zmianę hasła w usłudze Battle.net firmy Blizzard, wiadomość jest oryginalna i została wysłana z siedziby firmy Blizzard.

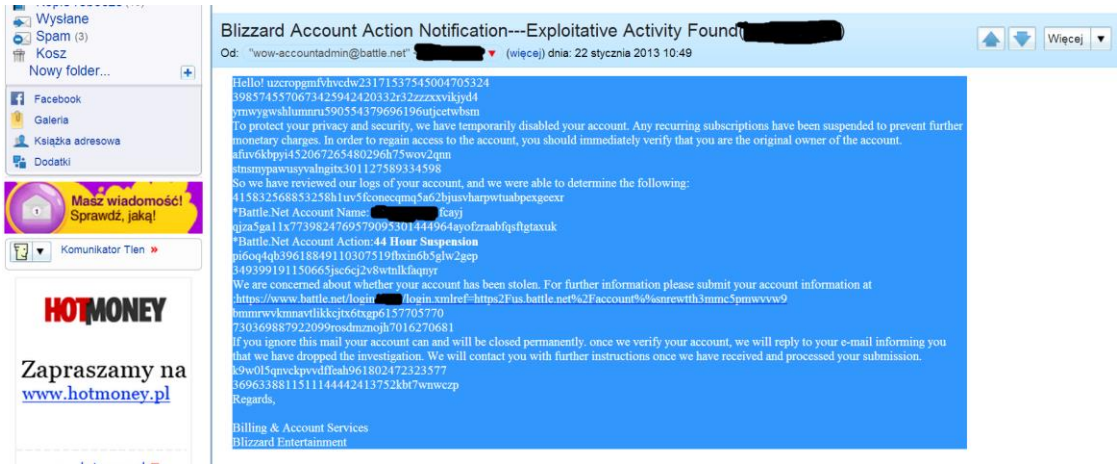


Ryc. 2 Przykład wiadomości wysłanej przez hakera podszywającego się pod pracownika firmy Blizzard, w celu zdobycia danych do konta Battle.net.



[14] W. Kasprzak: "*Ślady cyfrowe. Studium prawno-kryminalistyczne*", Warszawa 2015, s. 33

Ryc. 3 Ponownie oryginalna wiadomość od firmy Blizzard tym razem podświetlona przez autora. Podświetlenie nie wykazało żadnych ukrytych treści wiadomości mailowej.



Ryc. 4 Ponownie wiadomość od hakera, tym razem podświetlona w celu ujawnienia złośliwego kodu.[15]

Powyżej zamieszczone cztery zdjęcia przedstawiają przykładową próbę wyłudzenia danych poufnych metodą socjotechniczną[16]. Haker podszywając się pod pracownika firmy Blizzard używa podobnego adresu e-mail i formy oryginalnego listu. Trzeba zwrócić uwagę na trzy widoczne przesłanki świadczące o tym, iż wiadomość jest podejrzana. Pierwszą jest fakt wysłania do adresata (użytkownika gry World of Warcraft) wiadomości zawierającej link (URL), pod którym miał zweryfikować swoje dane. Firma Blizzard (właściciel usługi gry MMO World of Warcraft) wielokrotnie powtarza i zamieszcza w swoich regulaminach informację, że jej pracownicy nigdy nie żądają danych do konta ani innych poufnych informacji o swoich użytkownikach droga mailową. Druga przesłanką jest próba wywarcia na użytkownika presji czasowej wynoszącej 44 godziny. Po tym czasie konto może zostać zablokowane. Metoda taka jest klasyczną próbą oddziaływania na psychikę odbiorcy, starając się wzbudzić w nim niepokój i obawę o stan swojego dobra Internetowego. Wiele ofiar niestety ulega tej metodzie i wchodzą w linki niewiadomego pochodzenia, przestraszeni możliwością utraty danych. Nie spodziewają się natomiast, że właśnie padają ofiarą hakera. Trzecią przesłanką jest fakt ujawniony na ostatnim zdjęciu (ryc. 4). Wiadomość posiada ukryty kod, niewiadomego zastosowania. Możemy porównać, iż na pierwszym zdjęciu (ryc.2) wiadomość wygląda normalnie. Innym zastosowaniem omawianej techniki jest wysyłanie e-maila zawierającego informację, iż jakaś osoba jest w posiadaniu znacznej sumy pieniędzy, np. 25 mln dolarów, jednak by uzyskać dostęp do tych pieniędzy wymaga od adresata e-maila pomocy, która będzie polegać na udostępnieniu małej kwoty pieniędzy w celach manipulacyjnych lub danych personalnych i danych na temat karty kredytowej.

Drugą metodą mogącą posłużyć do kradzieży danych do konta bankowego jest zainfekowanie komputera ofiary złośliwym oprogramowaniem lub wykorzystanie bardziej zaawansowanych urządzeń, np. skanujących karty kredytowe. W tym przypadku możemy wyróżnić następujące najczęściej spotykane techniki:

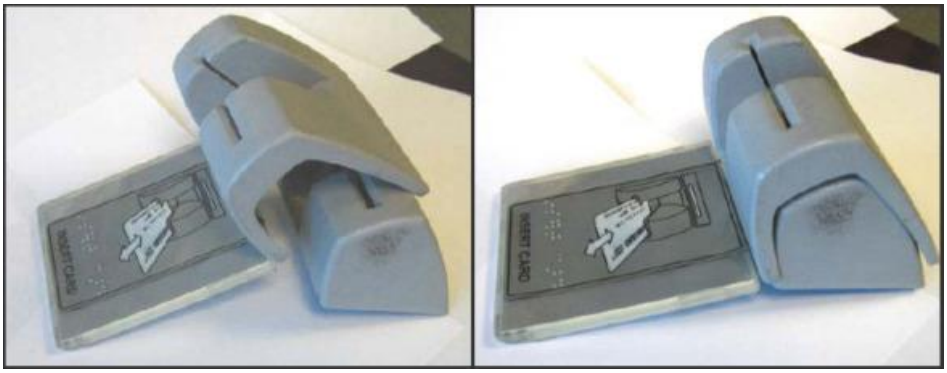
1. Koń Trojański - (znany także jako Trojan) - program, który podszywając się pod przydatną i użyteczną aplikację dla potencjalnego użytkownika, posiada tak naprawdę ukryte funkcje, które to pozwalają z kolei jego autorowi na przeprowadzanie nieautoryzowanych oraz niepożądanych czynności na maszynie swojej ofiary. Dla zachowania pozorów, niektóre konie trojańskie rzeczywiście oferują swojej ofierze przydatne funkcje, jednak użytkownik nie ma pojęcia, iż oprócz tych funkcji istnieje cały szereg innych postronnych procedur, poprzez które na pierwszy rzut oka „przyjazny" program jest niebezpiecznym narzędziem w rękach włamywacza (atakujący jest w stanie kierować działaniem trojana bez wiedzy użytkownika).
2. Fałszywe strony - technika polegająca na stworzeniu podrobionej strony usługi internetowej, np. strona logowania do systemu bankowego konta. Strona taka bliźniaczo przypomina swój oryginał i ma za zadanie zmylić użytkownika, by wprowadził tam swoje loginy i hasła. Strony takie mogą się znajdować często w

[15] materiały własne

[16] Socjotechnika - jedna z najczęstszych metod ataku z wykorzystaniem poczty elektronicznej. Haker stara się wpłynąć na umysł odbiorcy w taki sposób by uzyskać od samej ofiary potrzebne dane. Socjotechnika jest to psychologiczna metoda zdobywania informacji. Takim atakiem może być np mail, telefon lub inna forma zawiadomienia użytkownika danej usługi o pewnym wyimaginowanym problemie, jaki zaistniał. Haker podszywa się wówczas pod administratora lub pracownika firmy, w której konsument posiada swoje konto. Wysyłane maile najczęściej odnoszą się do faktu zaistniałego zagrożenia w stosunku do istniejącego konta gracza - użytkownika i wymagane jest natychmiastowe potwierdzenie danych poufnych. Haker najczęściej zamieszcza link do podrobionej strony, bliźniaczo podobnej do oryginalnej, na której użytkownik musi zalogować się na swoje konto. Dane oczywiście zostają przesłane na komputer hakera.

przysyłanych fałszywych e-mailach jako linki URL i na stronach internetowych podejrzanego pochodzenia. By uchronić się przed tego typu zagrożeniem można ręcznie wpisywać adresy strony docelowej banku w przeglądarce internetowej.

3. Urządzenia przestępcze - nowoczesne technologie, pozwalające przestępcom na wykorzystywanie bardzo wyrafinowanych metod popełniania czynów zabronionych z wykorzystaniem urządzeń cyfrowych. Do grupy urządzeń określanych jako „technologie przestępcze" możemy zaliczyć, np. nielegalne i nieautoryzowane czytniki kart magnetycznych, skanery kodów i banknotów, pluskwy, podsłuchy, keyloggery i inne urządzenia cyfrowe wykorzystywane w złej wierze. Najczęściej są to urządzenia będące nielegalnie podłączonymi i funkcjonującymi, na zasadzie „pasożyta", pod większe sprzęty cyfrowe. Można tutaj wyróżnić fałszywe czytniki kart bankowych montowane w bankomatach przez złodziei. Urządzenia z grupy przestępczych charakteryzują się najczęściej niewielkim rozmiarem, konstrukcją sprecyzowaną na wykonywanie ściśle określonych celów. Urządzenia takie posiadają zawsze pamięć masową w której przechowywane są skradzione dane lub nadajnik umożliwiający natychmiastowe wysyłanie przechwytywanych informacji wprost do komputera hakera.



Ryc. 5 Przykładowy skaner kart bankomatowych[17]

Liczba dokonywanych ostatnio włamań komputerowych, nazywanych przestępczością teleinformatyczną, a związanych bezpośrednio z hakerstwem - ma tendencję wzrostową[18]. Mimo że haking jako zjawisko subkulturowe w przeważającej większości spotykane jest wśród utalentowanej i myślącej nowoczesnymi kategoriami młodzieży, której nieobca jest technika komputerowa, to nie jest on wyłącznie domeną tej kategorii ludzi. Zajmują się nim również zawodowi informatycy, a co więcej jest to sfera zainteresowania zorganizowanych grup przestępczych o charakterze mafijnym[19]. Jednym z penalizowanych w polskim Kodeksie karnym przestępstw komputerowych jest, wspomniany wcześniej, haking (art. 267 § 1 k.k.). Polega on na włamaniu do systemu informatycznego i sieci komputerowej z pokonaniem ustanowionych zabezpieczeń, których zadaniem jest ochrona dostępu do przechowywanych i przetwarzanych informacji. Upowszechnienie Internetu spowodowało, że wiele komputerów i lokalnych sieci informatycznych zostało podłączonych do sieci publicznej, przez co stały się one narażone na włamania hakerów zlokalizowanych na przestrzenie całego globu[20]. Treść art. 267 § 1 k.k. w brzmieniu: *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*[21]. Pojęcie zabezpieczenia obejmuje wszelkie formy utrudniania dostępu do informacji, których likwidacja niesie za sobą wymóg specjalnej wiedzy albo posiadania dedykowanego urządzenia bądź kodu. W szczególności za zabezpieczenie uznać można hasło dostępu, program komputerowy pozwalający na odszyfrowanie zakodowanej informacji, dekoder. Co istotne, termin szczególne zabezpieczenie nie dotyczy jedynie kodowania informacji, ale obejmuje swoim zasięgiem również zabezpieczenia mechaniczne samego nośnika informacji, jak chociażby zamknięcie w sejfie[22]. Treść

[17] http://www.bootsnall.com/articles/10-04/atm-skimmers-how-to-protect-yourself.html, dostęp 17.02.2016r.
[18] por. L. Klander: "*Hacking proof - czyli jak sie bronić przed intruzami*", Warszawa, brak darty wydania, s. 304, por. P. Dziak, P. Figat, K. Kaczanowska, M. Sarna, J. Wownysz: "*Bezpieczne korzystanie z Internetu*", Warszawa 2012, s. 5, por. A. Korusiewicz: "*Zagrożenia w sieci Internet*", Warszawa 2007, s. 32, por. T. Jordan: "*Hakerstwo*", Warszawa 2011, s. 85
[19] B. Hołyst, op. cit., s. 82.
[20] A. Suchorzewska, op.cit., s. 211.
[21] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2015 r. poz. 1855).
[22] A. Suchorzewska, op.cit., s. 212.

wskazanego wyżej art. 267 § 1 k.k. dzieli posiadaczy komputerów na dwie grupy – tych, którzy stosują środki zabezpieczające, i tych, którzy ich nie stosują, przyznając ochronę grupie pierwszej[23].

Kolejnym penalizowanym w polskim Kodeksie karnym przestępstwem są oszustwa z wykorzystaniem kart płatniczych dokonywane z reguły z użyciem kart: zagubionych lub skradzionych, nieotrzymanych, otrzymanych na skutek fałszywych wniosków, podrobionych[24]. Pierwszy przypadek dotyczy sytuacji, w której karta nie została zastrzeżona wobec czego transakcja może dojść do skutku. Jeżeli sprawca znajdzie się w posiadaniu karty i kodu PIN ma możliwość wypłaty gotówki albo zrealizowania transakcji autoryzowanej podpisem. W przypadku kart nieotrzymanych transakcji dokonuje się wykorzystując karty wysyłane pocztą, które nie dotarły do adresata. Istotą oszustwa z użyciem kart płatniczych otrzymanych na skutek fałszywych wniosków jest natomiast wykorzystanie fałszywych dokumentów w celu uzyskania karty[25]. Fałszerstwa kart poza podrobieniem mogą mieć postać przerobienia, całkowitego fałszerstwa lub fałszerstwa elektronicznego. Z przerobieniem mamy do czynienia kiedy na oryginalnych kartach z zastosowaniem różnych metod, takimi jak działania mechaniczne i chemiczne, np. doklejenie, wytłoczenie, sprasowanie, zestruganie, wytrawienie, zmienia się numer karty, datę ważności i inne dane tę ważność ograniczające. Całkowitego fałszerstwa dokonuje się natomiast metodą tzw. białego plastiku, kiedy sfałszowana karta jest kawałkiem czystego plastiku z wytłoczonymi danymi, niezbędnymi do odbicia rachunku obciążeniowego, albo też kawałkiem plastiku z naniesionym wyłącznie paskiem magnetycznym z zapisanymi danymi. Istotą fałszerstwa elektronicznego jest z kolei zmiana zapisu na pasku magnetycznym bądź w pamięci mikroprocesora karty[26]. Kolejnym typem oszustwa z wykorzystaniem kart płatniczych jest tzw. skimming, polegający na kopiowaniu całej zawartości paska magnetycznego prawdziwej karty celem wykonania jej kopii. Specjalne urządzenie mocuje się przeważnie w bankomatach, w miejscu przeznaczonym na wprowadzenie kart (patrz ryc 5). W tego rodzaju przestępstwach używa się także dostępnych w Internecie oprogramowań komputerowych, właściwych dla konkretnego banku i typu karty płatniczej wyposażonej w numerację i zabezpieczenia, które służą do wygenerowania fałszywej karty. Dodatkowo odnotowuje się takie typy oszustw jak: przestępcze zawładnięcie konta i przestępcze wykorzystanie cudzego konta. Pojawiają się również zjawiska takie jak: kopiowanie kart na rachunkach obciążeniowych, bezprawne wykorzystanie numeru karty, użycie karty zgłoszonej jako utraconej, wyłudzanie towarów i usług przez legalnego użytkownika karty, włamania do systemów informatyczno – telekomunikacyjnych, mających doprowadzić do zdobycia dostępu do numerów kart, haseł, komunikatorów potwierdzających autoryzację, manipulację bankomatami, czy transakcje kartami dokonywane w Internecie[27]. W krajach wysoko rozwiniętych wzrost nadużyć związanych z kartami płatniczymi nastąpił pod koniec lat 80. Eksperci zauważają, iż nie powodują one wielkich strat jednostkowych, lecz niepokojące są ich rozmiary. Głównie odnosi się to do wzrostu zagrożeń związanych z kradzieżą, fałszowaniem oraz wypłatą pieniędzy na cudze karty płatnicze[28]. Fałszerstwa kart płatniczych penalizuje art. 310 § 1 k.k.[29].

Najcenniejszym zasobem współczesnego świata jest bez wątpienia informacja w formie danych, wiedzy i umiejętności. Pozwala ona nie tylko zarządzać teraźniejszością, ale też przewidywać przyszłość i poddawać analizie łączące je trendy. Z tego względu płaszczyzna ich bezpieczeństwa staje się tak ważnym aspektem[30]. Ewoluujące zagrożenia i pojawiające się nowe wyzwania wymuszają adaptowanie polityki, strategii i systemów bezpieczeństwa do nowych warunków. Bezpieczeństwo informacyjne dotyczące tak wielu dziedzin życia jak chociażby bezpieczeństwo ekonomiczne, polityczne czy społeczne, będzie trwałym elementem sfery bezpieczeństwa uczestników stosunków międzynarodowych, jak twierdzi K. Liedel, *aż po przysłowiowy „koniec historii"*[31]. We współczesnym świecie odpowiednia i skuteczna ochrona dostępu do systemów informatycznych stanowi kluczowy czynnik decydujący o bezpieczeństwie informacji. Odpowiedzialność za właściwy wybór i ustanowienie środków zabezpieczających pozostaje w gestii właścicieli systemów, ich zarządców bądź administratorów. A. Adamski wskazuje, iż środkom karnym przypada w tym zakresie zdecydowanie rola pomocnicza[32]. Zarówno praktyka śledcza jak i orzecznictwo sądowe wskazują na ograniczone możliwości ścigania sprawców przestępstw komputerowych. Głównym czynnikiem wpływającym na taki stan rzeczy jest specyfika tego rodzaju przestępstw, polegająca na ponadnarodowym charakterze, czyli transgranicznym działaniu sprawców, możliwości zdalnego ich działania oraz łatwości w kamuflowaniu swojego czynu. Wymienione elementy stwarzają ogromne trudności, zarówno wykrywcze jak i dowodowe. Ponadto

[23] Ibidem, s. 218.
[24] B. Hołyst, *Kryminalistyka*, wyd. IX zm., Warszawa 2007, s. 213.
[25] Ibidem, s. 213.
[26] B. Hołyst, *Kryminalistyka*, op. cit., s. 213-214.
[27] Ibidem, s. 214.
[28] J. W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne*, Warszawa 2008, s. 380.
[29] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2015 r. poz. 1855).
[30] K. Liedel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, Warszawa 2011, s. 437.
[31] Ibidem, s. 448.
[32] A. Suchorzewska, op.cit., s. 218.

charakterystyczne *modus operandi* sprawców przestępstw komputerowych, opierające się na niekonwencjonalnym sposobie ich działania jest nierozerwalnie związane z zastosowaniem nowych, równie nieszablonowych metod wykrywczych[33]. Ważnym jest by ofiary przestępstw komputerowych pamiętały, że ta grupa przestępstw jest ścigana wyłącznie na wniosek osoby pokrzywdzonej, za wyjątkiem ściganego z urzędu sabotażu komputerowego[34]. Hakerzy są w stanie bardzo szybko wykryć luki w potencjalnie bezpiecznym oprogramowaniu i wykorzystać je w celu nieautoryzowanego wejścia, kradzieży czy destrukcji plików. Nie istnieją skuteczne metody zabezpieczania systemów komputerowych w gospodarstwach domowych i państwowych instytucjach. Można jedynie rozwijać działania prewencyjne i nie pozwolić wyprzedzić się ciągłemu wyścigu zbrojeń na arenie cyberprzestrzeni[35].

[33] J. W. Wójcik, op. cit. s. 380.
[34] M. Sokół, R. Sokół*, Internet. Jak surfować bezpiecznie*, Gliwice 2005, s. 27.
[35] J. Kulesza, "*Ius internet*", Warszawa 2010, s. 82.