Anna Grobel-Kijanka[1]

Czynnik ludzki jako kluczowy element systemów bezpieczeństwa informacji

W dzisiejszym świecie informacja stanowi strategiczny zasób organizacji, a właściwa jej ochrona i wykorzystanie decydują o przewadze konkurencyjnej przedsiębiorstwa. Wraz z dynamicznym rozwojem technik informatycznych i powszechnym ich wdrożeniem do procesów biznesowych, systematycznie rośnie ilość dostępnych w sieciach komputerowych, w tym w Internecie, zasobów informacyjnych oraz usług świadczonych drogą elektroniczną. Jednocześnie nasilają się działania przestępcze skierowane na kradzież i nielegalne wykorzystanie danych. Skala oraz tempo ewoluujących zagrożeń bezpieczeństwa świadczą o tym, że każdy indywidualny użytkownik Internetu oraz każda instytucja gromadząca, przetwarzająca i przesyłająca dane ponosi ryzyko związane z ich kradzieżą. Do utraty danych dochodzi najczęściej nie z powodu „złamania" zabezpieczeń systemów informatycznych, ale z powodu nieświadomego i lekkomyślnego korzystania z sieci przez użytkowników. System bezpieczeństwa danych jest tak silny, jak jego najsłabsze ogniwo. Bazując na doświadczeniu sławnego hakera Kevina Mitnicka to „*czynnik ludzki jest piętą achillesową systemów bezpieczeństwa"*[2].

Niniejszy artykuł koncentruje się głównie na pozatechnicznym aspekcie bezpieczeństwa informacji związanym z brakiem odpowiedniej świadomości wśród użytkowników Internetu, co do istniejących zagrożeń i nieprzestrzegania przez nich zaleceń dotyczących bezpiecznego korzystania z systemów informatycznych. Jego celem jest ukazanie znaczenia czynnika ludzkiego jako źródła zagrożeń w systemach bezpieczeństwa informacji.

Rozważania teoretyczne wzbogacono opisem scenariuszy opartych na faktycznych zdarzeniach, przedstawiających przykładowe stosowane przez przestępców metody ataków i kradzieży danych wykorzystujące słabości ludzkiej natury. Wymienione zostały podstawowe zasady, których znajomość i prawidłowe stosowanie może uchronić przed kradzieżą informacji.

---

[1] Autorka pracuje w Wyższej Szkole Zarządzania i Bankowości w Krakowie jako wykładowca przedmiotów informatycznych oraz instruktor Akademii Sieci Komputerowych CISCO. Jednocześnie pełni funkcję zastępcy dyrektora działu IT.

[2] Mitnick K., W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła, Helion 2003*, s. 15.

Ewolucja zagrożeń

Sposób wymiany informacji ulega dynamicznym przemianom. 3,03 mld ludzi, czyli blisko 42% populacji korzysta obecnie z Internetu[3]. Aż trudno uwierzyć, że w Polsce zaledwie ćwierć wieku temu przesłano pierwszą wiadomość e-mail, a dzisiaj ponad 2/3 Polaków (25,7 mln) to aktywni internauci, z czego więcej niż połowa zarejestrowana jest na portalach społecznościowych. Świat komunikuje się coraz częściej za pomocą urządzeń mobilnych, statystycznie co drugi człowiek ma telefon komórkowy. Na 100 Polaków przypada 150 aktywowanych kart SIM, 44% obywateli naszego kraju jest w posiadaniu smartfona. 13 mln rodaków aktywnie korzysta z bankowości internetowej, co czwarty z nich używa serwisu banku na urządzeniu mobilnym[4]. Zarówno przedsiębiorstwa, jak i użytkownicy indywidualni, w coraz większym stopniu uzależnieni są od sprawnego i bezpiecznego działania systemów informatycznych.

Gwałtownie rośnie ilość dostępnych w Internecie zasobów informacyjnych. Ocenia się, że każdego dnia świat generuje 2,5 eksabajta nowych informacji[5]. Już w latach 40. XX wieku laureat Nagrody Nobla w dziedzinie ekonomii Friedrich von Hayek postrzegał informację jako kategorię ekonomiczną. „*Każda właściwie jednostka ma pewną przewagę nad wszystkimi innymi, ponieważ posiada jedyne w swoim rodzaju informacje, które można z powodzeniem wykorzystać*”[6].

W czasach, w których informacja stała się towarem, działania przestępcze w Internecie stały się atrakcyjnym źródłem zysków. Według szacunków raportu opracowanego przez amerykańskie Centrum Studiów Strategicznych i Międzynarodowych CSIS, ekonomiczne skutki oddziaływania przestępczości internetowej w skali światowej wynoszą ponad 400 mld USD rocznie[7], co stanowi blisko 1/5 wartości generowanej przez Internet. Gdyby cyberprzestępczość była gospodarką, zajęłaby 27. miejsce zaraz za Norwegią, której wielkość PKB szacowana jest przez Międzynarodowy Fundusz Walutowy w 2015 r. na 421 mld USD[8] (Polska w rankingu tym zajmuje 23. miejsce). Największe straty powodują ataki hakerskie obejmujące blokowanie zasobów, włamania, kradzieże, w tym rabunek poufnych danych

[3] Kemp S., *Digital, Social, and Mobile in Apac 2015*, s. 7.
[4] Związek Banków Polskich, NetB@nk – Raport: *Bankowość internetowa i płatności bezgotówkowe, IV kwartał 2014 r.*, s. 6.
[5] Płoszajski P., *Big Data: nowe źródło przewag i wzrostu firm* [w:] E-mentor nr 3 (50), 2013.
[6] Hayek F.A., *The Use of Knowledge in Society*, www.virtualschool.edu/mon/Economics/HayekUseOfKnowledge.html.
[7] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, s. 2.
[8] *World Economic Outlook Database, April* 2015, www.imf.org [dostęp: 18.06.2015].

biznesowych, niszczenie informacji, wyłudzenia i oszustwa, piractwo komputerowe. Za koszty uznać należy również środki i czas poświęcone na rozwiązywanie problemów.

Publikowane raporty stanu bezpieczeństwa sieciowego wskazują na ciągle rosnącą liczbę zagrożeń. Każda firma, każdy indywidualny użytkownik może stać się celem coraz bardziej wyrafinowanej formy ataku[9]. Niezwykle sugestywny obraz zagrożeń można znaleźć na stronie map.ipviking.com, która wyświetla w czasie rzeczywistym globalną mapę różnych typów ataków, ich źródła oraz cele.

Zagrożenia nie omijają niestety naszego kraju. Według raportu Zespołu CERT Polska[10], który monitoruje i analizuje przypadki naruszenia bezpieczeństwa rodzimej sieci, najważniejszym i najbardziej niepokojącym trendem w 2014 roku był wzrost ataków na użytkowników indywidualnych i klientów korporacyjnych bankowości internetowej.

Nieświadomość użytkowników co do istniejących zagrożeń skutkuje podatnością na wykonywanie zagrażających bezpieczeństwu operacji.

Brak ochrony prywatności i kradzież tożsamości

Globalne straty związane z naruszaniem bezpieczeństwa danych osobowych wyceniane są na 160 mld dolarów[11]. Bardzo często pracownicy przedsiębiorstw oraz użytkownicy indywidualni sami narażają się na niebezpieczeństwo, beztrosko rezygnując z ochrony własnej oraz firmowej prywatności. Wiele osób nie przestrzega podstawowych zasad bezpieczeństwa sieciowego. 31% włamań w 2014 roku było efektem stosowania zbyt prostych haseł. 61% użytkowników korzysta z tego samego hasła do wielu usług internetowych[12]. Co czwarty użytkownik dane dostępowe do serwisów internetowych zapisuje automatycznie w swoim komputerze[13].

Należy pamiętać, że już poprzez samo przeglądanie stron internetowych użytkownik pozostawia za sobą wyraźny ślad. Wszechobecne „ciasteczka", często zbyt pochopnie akceptowane na wszystkich odwiedzanych stronach, umożliwiają stworzenie „profilu użytkownika" i śledzenie jego zachowań (najczęściej po to, aby dostarczać mu takich treści, które mogłyby go zainteresować). Coraz częściej dostęp do szczegółowych, ciekawych

[9] Deloitte, *Cyberodporność w świecie ewoluujących zagrożeń. Nowe drogi w bezpieczeństwie informacji*, s. 17.
[10] CERT Polska, *Raport 2014*, s. 10.
[11] Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime*, s. 3.
[12] CHIP, 03/2015, s. 7.
[13] Wilk A., *Kradzież tożsamości, Raport z badań*, 2014, s. 18.

informacji na stronach internetowych wymaga rejestracji, portale internetowe powszechnie zachęcają do wypełniania formularzy i ankiet z podaniem danych osobowych. Ceną ich ujawnienia może być spłata niezaciąganych kredytów, PESEL i numer dowodu osobistego wystarczają bowiem do zakupów na kredyt przez Internet.

Przykładowy scenariusz kradzieży tożsamości, czyli bezprawnego wejścia w posiadanie danych osobowych i nieuprawnionego ich wykorzystania, może być następujący: oszuści wystawiają na różnych portalach atrakcyjne oferty pracy, czasem żądają od kandydatów skanu dowodu, aby rzekomo zweryfikować ich niekaralność. Podając wyłudzone informacje, oszuści zakładają bankowe konto internetowe tzw. „słupa". Aby konto stało się aktywne banki wymagają dla potwierdzenia tożsamości osoby, przelewu z innego jej konta. Oszuści nakłaniają więc ofiarę na przelanie symbolicznej złotówki ze swojego konta na wskazany rachunek np. pod pretekstem chęci uzyskania numeru konta dla przyszłych wypłat. Jeden rachunek „na słupa" może posłużyć do wyłudzenia pożyczek w paru firmach oferujących w Internecie „chwilówki". Przestępcy mając kontrolę nad jednym kontem, mogą otworzyć kolejne rachunki w bankach, które dają możliwość autoryzacji za pomocą przelewu z innego banku. Poprzez generowanie obrotów na kontach ofiar oszuści mogą zdobyć zaufanie banków i w ten sposób wyłudzić wysokie kredyty. W zeszłym roku udaremniono próby wyłudzeń kredytów o łącznej wartości 400 mln zł[14].

Duże zagrożenie dla bezpieczeństwa danych stwarza nierozważne korzystanie z portali społecznościowych, gdzie można znaleźć dobrowolnie ujawnione, prywatne dane, osobiste zdjęcia, z których nie trudno wywnioskować, jaki jest status materialny publikującej je osoby. Fotografie publikowane wprost z podróży są informacją, że dom może być bez opieki – okazja czyni złodzieja. Pracownicy przedsiębiorstw nieostrożnie ujawniają informacje dotyczące firm, w których pracują – często informacje poufne (plany marketingowe, szczegóły rozwiązań technicznych, wyniki prac badawczych, a także informacje, o których mowa w ustawie o ochronie informacji niejawnych), które mogą być bezpardonowo wykorzystane przez wrogą konkurencję. Udostępniane informacje mogą być też użyte przez przestępców w atakach socjotechnicznych. Korzystanie z serwisów społecznościowych jest czynnikiem ryzyka, którego nie można pominąć w polityce bezpieczeństwa organizacji.

[14] Bednarek M., *I ty możesz zostać słupem* [w:] Gazeta Wyborcza, [dostęp: 14.05.2015].

Ataki socjotechniczne

Phishing należy do najpopularniejszych sposobów kradzieży, w którym stosowane są elementy socjotechniki. Złodzieje perfidnie wyłudzają dane podszywając się pod banki, instytucje finansowe, firmy kurierskie, telekomunikacyjne, sklepy internetowe. Przestępcy preparują wiadomości, w których udając legalną instytucję proszą o podanie poufnych informacji, następnie rozsyłają je masowo pocztą elektroniczną do wszystkich użytkowników, których adresy e-mail udało im się pozyskać. Przykładowo, aby zdobyć m. in. numer konta, PIN do karty, podszywali się pod Ministerstwo Finansów i wysyłali wiadomość e-mail dotyczącą rzekomego zwrotu podatków wraz z formularzem do wypełnienia.

Rysunek 1. Przykład *phishingu*

Źródło: Ministerstwo Finansów, www.mf.gov.pl/ministerstwo-finansow/wiadomosci/komunikaty, publikacja: 17.12.2014, [dostęp: 18.06.2015].

Innym przykładem *phishingu* jest rozsyłanie *spamu* ze złośliwym oprogramowaniem. Przestępcy w zręczny sposób starają się nakłonić ofiarę do otwarcia przesłanego w załączniku pliku przekonując np., że przesyłają fakturę, list przewozowy lub inny ważny dokument. Często wiadomości rozsyłane przez oszustów zawierają odnośniki, kliknięcie których przekierowuje na podstawione strony do złudzenia przypominające serwisy legalnych instytucji – jeżeli użytkownik wprowadzi tam poufne dane, są one przechwytywane przez przestępców. Fałszywe strony zawierają też często odnośniki do złośliwego oprogramowania.

Dziennie wysyłanych jest 28 mld niechcianych e-maili, czyli statystycznie 4 do każdego mieszkańca Ziemi. Według statystyk firmy Symantec w szczytowym momencie 2014 roku w serwisach społecznościowych znajdowało się 30 tys. odnośników do sfałszowanych stron[15].

W atakach typu *spear phishing* oszuści, zamiast rozsyłać wiadomości do milionów przypadkowych użytkowników, starannie dobierają swoje ofiary. Atak poprzedza analiza dostępnych informacji dotyczących potencjalnych ofiar. Przykładowo w 2014 r. celowo wybrani pracownicy firm z sektora energetycznego, którzy mieli zamiar wziąć udział w konferencjach naukowych, otrzymywali fałszywe wiadomości e-mail ze specjalnie zmodyfikowanymi dokumentami, które informowały o programie imprez. Otwarcie takiego pliku skutkowało pobraniem i instalacją groźnych wirusów, które umożliwiały atakującym przejęcie kontroli nad komputerem ofiary i kradzież poufnych danych biznesowych[16]. Skuteczność ukierunkowanych ataków wykorzystujących informacje dostępne w serwisach społecznościowych wzrosła do 72% (z 15%, kiedy danych tych nie analizowano)[17].

Trudną do wykrycia odmianą *phishingu* jest *pharming*, polegający na modyfikowaniu ustawień serwera DNS (ang. *Domain Name Server*). Ofiara ataku mimo wpisania prawidłowego adresu strony internetowej, zostaje przekierowana na fałszywą stronę, celem przejęcia wpisywanych tam haseł, numerów kart kredytowych i innych poufnych danych.

Najbardziej zaawansowane informatyczne systemy ochrony danych nie są w stanie zapobiec kradzieży, gdy zawiedzie czynnik ludzki. W maju 2015 r. padł rekord wyłudzenia 3,7 mln złotych. Niechlubnym rekordzistą okazał się Podlaski Zarząd Dróg Wojewódzkich, który uwierzył w fałszywe pismo o zmianie numeru rachunku i przelał pieniądze na podstawione konto bankowe.

Złośliwe oprogramowanie

Niektóre serwisy powstają w Internecie tylko po to, by wyciągnąć dane użytkowników i/lub wymusić opłaty. Użytkownicy beztrosko korzystają z serwisów oferujących pirackie treści: oprogramowanie, filmy, gry. Często jednak, aby dotrzeć do pobierania tych plików, trzeba pokonać liczne zainfekowane wirusami strony, ominąć niebezpieczne reklamy i fałszywe oferty. Kilka kliknięć może kosztować – oprócz opłaty za „ściągany towar" –

[15] Symantec, *Internet Security Threat Report* v. 20, 2015, s. 57.
[16] CERT Polska, *Raport 2014*, s. 18.
[17] Kaczmarek A., *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, s. 52.

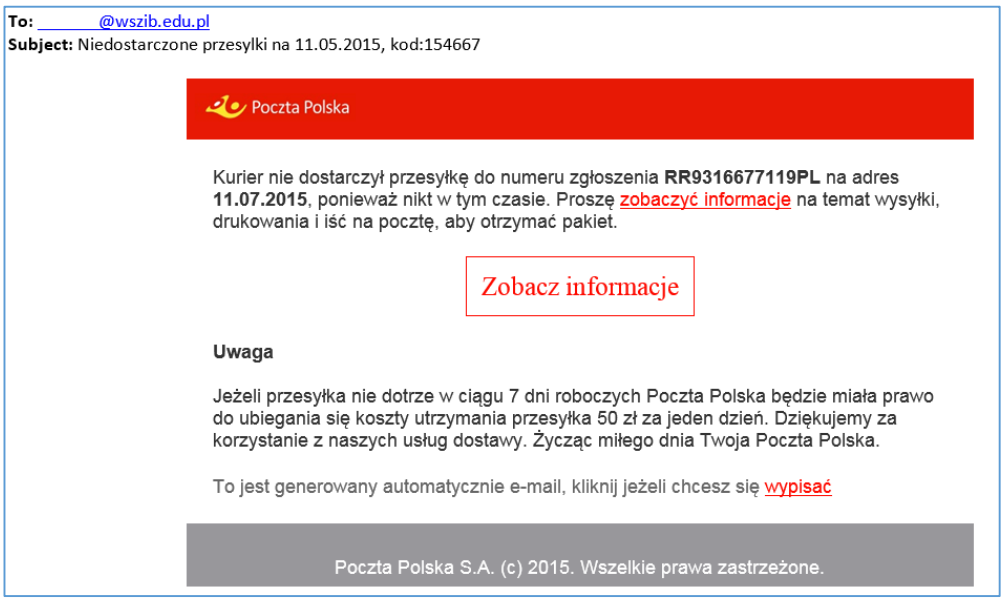
również comiesięczne rachunki za niechciane usługi (horoskopy, poradniki, muzykę), a często ich efektem jest instalacja złośliwego oprogramowania.

Każdego dnia powstaje blisko 1 mln nowych sygnatur złośliwych aplikacji[18]. Według szacunków cytowanego już raportu CERT, dziennie w Polsce zarażanych jest 280 tys. komputerów[19]. Coraz więcej typów wirusów, zaprojektowanych jest tak, aby atakować urządzenia mobilne. Najpopularniejszą metodą zarażania polskich internautów są zainfekowane załączniki w atakach socjotechnicznych.

Programy do wspomagania ataku na bezpieczeństwo danych stają się coraz bardziej wyrafinowane. Tzw. *exploity* wykorzystują błąd programistyczny występujący w oprogramowaniu komputera w celu przejęcia kontroli nad działaniem całego systemu operacyjnego lub wybranego procesu. *Keyloggery* rejestrują znaki wprowadzane przez użytkownika, dzięki czemu mogą przechwycić poufne dane logowania do systemów. Zagrożeniem dla klientów bankowości elektronicznej jest m. in. trojan *Retefe*, który konfiguruje w systemie Windows nowy serwer DNS, instaluje certyfikat bezpiecznego połączenia SSL[20], po czym przekierowuje próby połączenia się z bankiem na sfałszowaną, szyfrowaną witrynę oszustów. Niebezpieczny jest również wirus *Banatrix*, podmieniający numer konta klienta na numer rachunku przestępców podczas operacji *kopiuj-wklej*. W 2015 r. polska sieć została zalana falą *phishingu* z załącznikami lub odnośnikami do złośliwego oprogramowania, którego przykładem jest *CryptoLocker*, szyfrującego pliki na dysku ofiary. Jeżeli właściciel zarażonego komputera nie zapłaci okupu w określonym przez oszustów czasie, klucz służący odszyfrowaniu plików ulega zniszczeniu i użytkownik bezpowrotnie traci dostęp do danych.

[18] Symantec, *Internet Security Threat Report v. 20*, 2015, s. 7.
[19] CERT Polska, *Raport 2014*, s. 41.
[20] Certyfikat SSL (ang. *Secure Socket Layer*) zapewnia zachowanie poufności danych przesyłanych drogą elektroniczną dzięki zastosowaniu szyfrowania komunikacji.

Rysunek 1. Zainfekowane wirusem *CryptoLockera* wiadomości e-mail, rzekomo nadawane przez Pocztę Polską



Źródło: opracowanie/doświadczenie własne.

Zarażone urządzenia mobilne i komputery są wykorzystywane przez oszustów do dalszych ataków (np. wysłanie spamu, DDoS[21]) lub przestępcy czerpią z nich zyski poprzez przejęcie i sprzedaż poufnych danych tam zapisanych, wymuszenia okupu, kradzież z internetowych kont bankowych, itp. Coraz bardziej popularne staje się używanie osobistych urządzeń przenośnych do przetwarzania kluczowych danych firmowych. Przejęcie kontroli nad prywatnym urządzeniem pracownika może skutkować kradzieżą lub zniszczeniem strategicznych informacji biznesowych.

Aby choć częściowo zabezpieczyć się przed instalacją złośliwego kodu należy aktualizować na bieżąco system operacyjny i oprogramowanie, używać sprawdzonego programu antywirusowego, nie otwierać wiadomości e-mail, a tym bardziej załączników, od nieznanych nadawców. Nie należy korzystać z konta z uprawnieniami administracyjnymi (za wyjątkiem instalowania aplikacji ze sprawdzonych źródeł). Zalecane jest możliwie częste archiwizowanie danych.

[21] DDoS (ang. *Distributed Denial of Service*) – atak na system komputerowy lub usługę sieciową przeprowadzany równocześnie z wielu komputerów w celu uniemożliwienia działania poprzez zablokowanie wszystkich wolnych zasobów.

W jaki sposób przestępcy „wyprowadzają" pieniądze z bankowych kont internetowych?

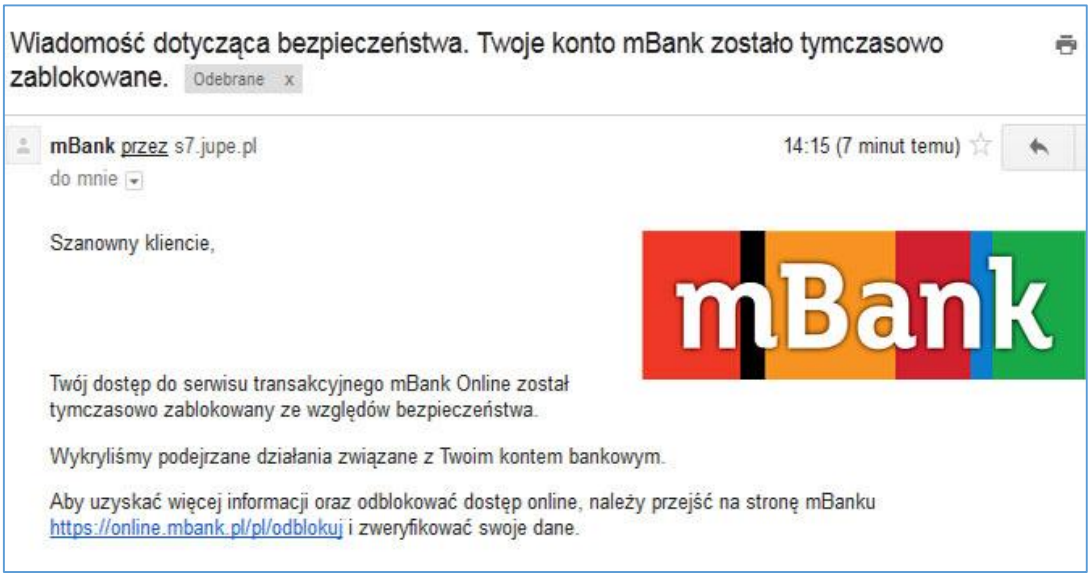
Sposoby działania przestępców ukierunkowane na kradzież w sektorze finansowym często wyznaczają trendy w metodach ataków na bezpieczeństwo informacji w instytucjach biznesowych innych branż. Warto budować świadomość zagrożeń śledząc i analizując przypadki naruszenia bezpieczeństwa w bankowości internetowej.

Dostępu do serwisu bankowego bronią najczęściej identyfikator, hasło oraz narzędzia autoryzacji transakcji. Aby więc wykraść pieniądze klienta banku, trzeba sforsować przeszkody autoryzacji. Opisywane scenariusze pokazują niektóre sposoby, którymi posługują się oszuści.

Scenariusz I

1. Przestępca przesyła wiadomość e-mail.

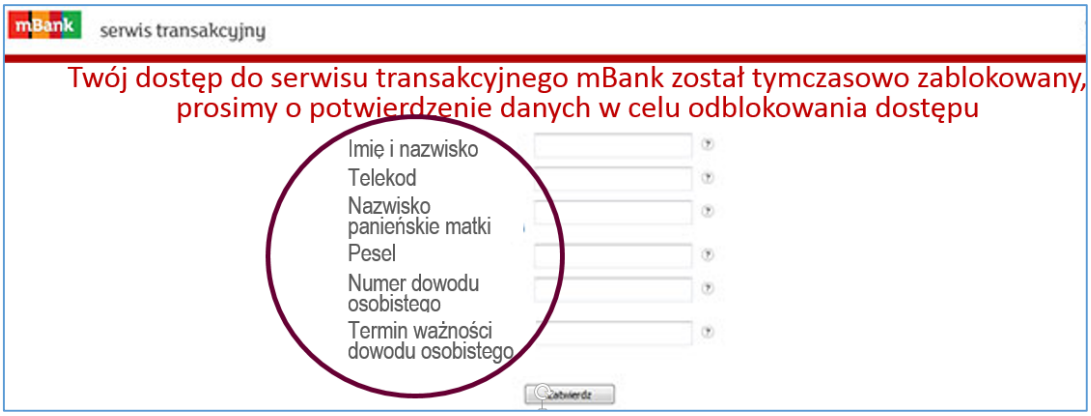
Rysunek 3. Wiadomość pochodząca rzekomo od banku



Źródło: www.komputerswiat.pl/nowosci/bezpieczenstwo/2015/07/falszywe-maile-z-mbanku-uwaga.aspx, [dostęp: 18.06.2015].

2. Użytkownik, który kliknie w link, zostaje przekierowany na fałszywą stronę serwisu internetowego banku. Po zalogowaniu identyfikator i hasło, trafiają w ręce złodzieja.
3. Pojawia się prośba o podanie dodatkowych danych.

Rysunek 4. Spreparowana strona serwisu bankowego



Źródło: www.komputerswiat.pl/nowosci/bezpieczenstwo/2015/07/falszywe-maile-z-mbanku-uwaga.aspx, [dostęp: 18.06.2015].

Przestępca będąc w posiadaniu powyższych informacji mógł zadzwonić na infolinię banku, a za jej pośrednictwem wykonać przelew na dowolne konto.

Scenariusz II

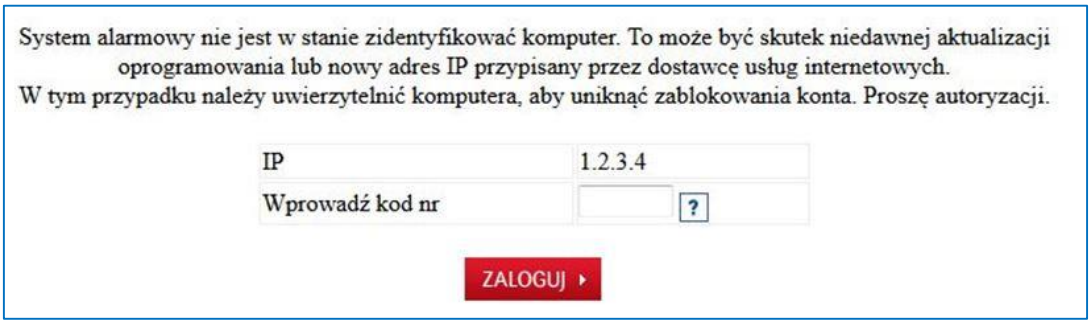
1. Przestępca instaluje złośliwe oprogramowanie w komputerze ofiary. Przechwytuje wpisywany podczas logowania klienta identyfikator oraz hasło.
2. Oszust podstawia klientowi fałszywą stronę informującą o konieczności zainstalowania na telefonie komórkowym oprogramowania, rzekomo podnoszącego poziom bezpieczeństwa.
3. Złodziej wysyła klientowi SMS z linkiem do instalacji wirusa.
4. Po infekcji urządzenia mobilnego oszust przejmuje nad nim kontrolę (również nad hasłami SMS niezbędnymi do autoryzacji transakcji). Przelewa pieniądze na rachunki „słupów".

W przypadku bankowości mobilnej działającej w pełnej funkcjonalności wystarczy przejąć kontrolę nad jednym urządzeniem klienta, aby dokonać kradzieży z jego konta.

Scenariusz III

1. Złodziej instaluje na komputerze ofiary złośliwe oprogramowanie, następnie zdobywa login i hasło do serwisu banku.
2. Oszust wyświetla na ekranie ofiary żądanie podania kodu jednorazowego, podając zmyślone uzasadnienie.

Rysunek 5. Przykład fałszywego komunikatu, który może pojawiać się użytkownikom logującym się do serwisu internetowego banku z zainfekowanego komputera



Źródło: www.pkobp.pl/bankowosc-elektroniczna/ipko/bezpieczna-bankowosc/uwaga-na-nowe-zagrozenia-w-sieci, [dostęp: 18.06.2015].

3. Z użyciem kodu przestępca definiuje konto „słupa" jako odbiorcę zdefiniowanego i przelewa na nie pieniądze ze wszystkich rachunków. Przelewy wewnętrzne zazwyczaj nie wymagają dodatkowej autoryzacji.

Scenariusz IV

1. Złodziej, który znajdzie lukę w zabezpieczeniach routera bezprzewodowego klienta[22], przejmuje nad nim kontrolę i zmienia konfigurację serwera DNS[23].
2. Oszust przekierowuje ruch na swój własny serwer i wyświetla użytkownikowi fałszywe strony.
3. Podszywając się pod oficjalną stronę banku uzyskuje dane podawane przez klienta podczas logowania.
4. Wyświetla żądanie do autoryzowania kodem SMS fałszywej transakcji.

Przesłany SMS potwierdza w rzeczywistości utworzenie odbiorcy zdefiniowanego do wyprowadzenia pieniędzy.

Scenariusz V

1. Przestępca instaluje złośliwe oprogramowanie *Banatrix* w komputerze ofiary.
2. W momencie, w którym klient wprowadza do formularza przelewu numer rachunku na zasadzie *kopiuj-wklej*, trojan podmienia numer konta ze schowka na numer rachunku złodzieja. Klient autoryzuje przelew na podstawione konto.

[22] Można sprawdzić zabezpieczenia własnego routera na stronie: cert.orange.pl/modemscan.
[23] niebezpiecznik.pl/post/stracil-16-000-pln-bo-mial-dziurawy-router-prawie-12-miliona-polakow-moze-byc-podatnych-na-ten-atak, [dostęp: 2015-06-17].

Banki zgodnie z oczekiwaniami klientów, żeby było coraz łatwiej, wygodniej i szybciej, niestety ułatwiają złodziejom działanie. Przestępcy w pierwszej kolejności kierują się tam, gdzie jest najmniej przeszkód do sforsowania. Nie bez powodu najwięcej jest ataków na klientów banków, które stosują niemaskowany identyfikator i hasło, brak dodatkowego uwierzytelniania, stosowanie tego samego, niezmiennego hasła przy logowaniu. Wykrycie nowego sposobu włamań powinno skutkować natychmiastowym wprowadzeniem zabezpieczeń w systemach chroniących klientów. Tymczasem część banków poprzestaje na publikowaniu komunikatów ostrzegających.

Podsumowanie

Postępująca dynamicznie ewolucja zagrożeń bezpieczeństwa zmusza do ciągłego podnoszenia stanu wiedzy w zakresie ochrony informacji. Na celowniku przestępców w pierwszej kolejności znajdują się ludzie, będący najsłabszym ogniwem systemów bezpieczeństwa. Podatność na ataki, zwłaszcza socjotechniczne, zagraża każdemu człowiekowi. Żeby ustrzec się przed zagrożeniami bezpieczeństwa danych, należy przede wszystkim uzmysławiać sobie ich istnienie i zachować szczególną ostrożność. W firmach należy budować w świadomości pracowników obraz współodpowiedzialności za bezpieczeństwo gromadzonych, przetwarzanych i przesyłanych danych. Wymagany jest również jasny i spójny system regulacji wewnętrznych w zakresie bezpieczeństwa informacji. Istotnym aspektem jest stałe monitorowanie i analizowanie publikowanych danych dotyczących naruszania bezpieczeństwa, współdziałanie i wymiana doświadczeń różnych organizacji.

Bibliografia

Bednarek M., *I ty możesz zostać słupem* [w:] Gazeta Wyborcza, 14.05.2015.

Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II*, intelSecurity, Santa Clara 2014.

CERT Polska, *Raport 2014*, NASK, Warszawa 2014.

CHIP, 03/2015.

Deloitte, *Cyberodporność w świecie ewoluujących zagrożeń. Nowe drogi w bezpieczeństwie informacji*, 2013.

Hayek F.A., *The Use of Knowledge in Society*, www.virtualschool.edu/mon/Economics/HayekUseOfKnowledge.html [dostęp:18.06.2015].

Kaczmarek A., *ABC zagrożeń bezpieczeństwa danych osobowych w systemach teleinformatycznych*, GIODO, Warszawa 2009.

Kemp S., *Digital, Social, and Mobile in Apac 2015*, We Are Social & IAB Singapore 2015.

Mitnick K., Simon W.L., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion, Gliwice 2003.

niebezpiecznik.pl/post/stracil-16-000-pln-bo-mial-dziurawy-router-prawie-12-miliona-polakow-moze-byc-podatnych-na-ten-atak [dostęp:18.06.2015].

Płoszajski P., *Big Data: nowe źródło przewag i wzrostu firm* [w:] E-mentor nr 3 (50).

Symantec, *Internet Security Threat Report v. 20*, Mountain View 2015.

Wilk A., *Kradzież tożsamości, Raport z badań*, Fellowes, 2014.

World Economic Outlook Database, April 2015, www.imf.org [dostęp:18.06.2015].

www.mf.gov.pl/ministerstwo-finansow/wiadomosci/komunikaty 2014.12.17 [dostęp:18.06.2015].

Związek Banków Polskich, NetB@nk – Raport: *Bankowość internetowa i płatności bezgotówkowe, IV kwartał 2014 r.*, zbp.pl/public/repozytorium/wydarzenia/images/marzec_2015/konf/Netbank_Q4_2014v3.pdf [dostęp:18.06.2015]