PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1091 — 2005
Finanse i rachunkowość – teoria i praktyka

Małgorzata Solarz

Akademia Ekonomiczna we Wrocławiu

BEZPIECZEŃSTWO BANKOWOŚCI INTERNETOWEJ

1. Wstęp

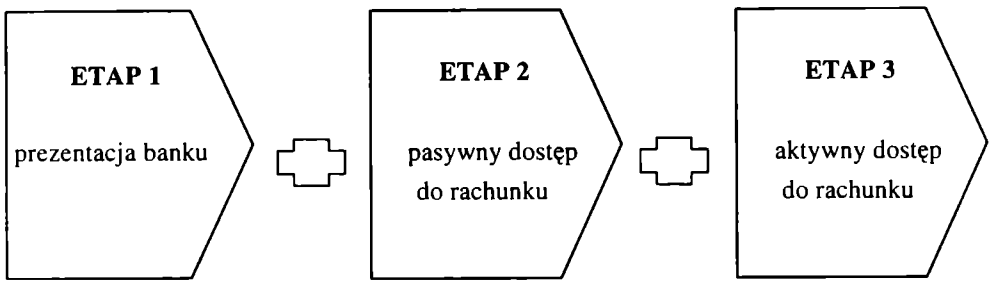
Bankowość internetowa oznacza usługi bankowe, przy których świadczeniu kontakt między bankiem a klientem odbywa się za pośrednictwem Internetu z wykorzystaniem komputera osobistego klienta. W Polsce pierwsze konto internetowe zostało założone 14 października 1998 r. w Powszechnym Banku Gospodarczym SA – Grupa Pekao SA w Łodzi [11, s. 27]. Od tamtej pory dynamicznie zwiększała się liczba internetowych rachunków bankowych, tak że na koniec czerwca 2004 r. było ich już 2,7 mln. Wśród liderów bankowości internetowej jest m.in. mBank – BRE Bank SA, pierwszy bank, który rozpoczął obsługę klientów wyłącznie za pośrednictwem Internetu i telefonu. W połowie 2004 r. obsługiwał on 780 tys. osób – niemal dwa razy więcej niż Bank Zachodni WBK SA, z którego usług korzystało 343,7 tys. osób. Kolejną pozycję zajął Inteligo – PKO BP SA z 311,70 tys. klientów [5].

Według wyników badań przeprowadzonych na toruńskim Uniwersytecie Mikołaja Kopernika posiadaczy internetowych kont bankowych byłoby zapewne jeszcze więcej, gdyby nie brak zaufania i poczucia bezpieczeństwa odczuwany podczas komunikowania się z instytucją bankową przez stronę www. Aż 65% ankietowanych pracowników banków wskazało na to zagrożenie jako na jedną z głównych barier rozwoju bankowości internetowej w Polsce [13]. Klienci obawiają się, że informacje o ich rachunkach oraz dane dotyczące zlecanych operacji, wykonywane z wykorzystaniem kanałów elektronicznych, mogą zostać podejrzane, przechwycone lub zmodyfikowane przez przestępców. Wśród zagrożeń dotyczących bankowości internetowej za najważniejsze można uznać [16, s. 24]:

- *cracking*: zgadywanie/łamanie/rozszyfrowywanie haseł dostępowych, algorytmów szyfrujących, kluczy publicznych i prywatnych,
- *sniffing*: podglądanie, podsłuchiwanie, np. za pomocą programu *packet sniffer*, umożliwiającego wgląd do treści pakietu do kabla, i oczekiwanie na dane przekazywane np. analizatorom sieci,
- *spoofing*: badanie sieci, np. przez aktywne podpięcie do kabla (tj. wpuszczanie do sieci) danych i poleceń, np. symulowanego protokołu komunikacyjnego, podszywanie się pod kogoś poprzez fałszywy adres internetowy i uzyskanie dzięki temu nielegalnego dostępu do danych,
- *back door* („tylne drzwi"): wejście do systemu w inny sposób niż przez logowanie, np. przez pocztę elektroniczną lub dzięki zainstalowaniu odpowiedniego oprogramowania, w celu podsłuchiwania wprowadzanych na klawiaturze znaków, co pozwala uzyskać hasło jeszcze przed jego zaszyfrowaniem,
- wprowadzenie „koni trojańskich", tj. obiektów pozornie niewinnych, a tak naprawdę przeznaczonych do uruchomienia działań destrukcyjnych na komputerze, na którym się znajdują (trojany są zaszywane w listach poczty elektronicznej, w plikach bat, com, exe, pseudotekstowych, zawierających wykonywalne skrypty, plikach rozpoznawanych jako *screen saver*).

Często spotykanym skutkiem działania oszustów, które można zakwalifikować do trzeciej z ww. grup zagrożeń, jest kradzież witryny internetowej. Polega to na dokonaniu takich zmian w komputerach obsługujących nazwy serwerów internetowych, aby próby wywołania strony www banku skutkowały zgłoszeniem się zupełnie innego serwisu, często prezentującego obraźliwe treści i obrazy wobec oryginalnego adresata [12, s. 222]. Jeżeli napastnik ograniczy się do tego rodzaju działań, to jedynie ośmieszy daną instytucję bankową, jednocześnie podważając jej wiarygodność. Gorzej, gdy oszust, tworząc imitację strony bankowej, zdobędzie dane od nieświadomych tego klientów.

Wszystkie banki, a więc także internetowe, są instytucjami zaufania publicznego, dlatego też szczególna uwaga należy się ich bezpieczeństwu. Stosują one wiele rodzajów zabezpieczeń odpowiednio do stopnia wykorzystania przez nie Internetu jako alternatywnego kanału dystrybucji usług bankowych. Wspomniane medium telekomunikacyjne banki włączają do swej oferty etapami, zaczynając od stworzenia strony www, służącej głównie celom informacyjnym i promocyjnym, przez udostępnianie coraz to bardziej złożonych usług, a kończąc na pełnej wirtualizacji oferty (rys. 1).



Rys. 1. Włączanie Internetu do działalności banku
Źródło: opracowanie własne.

Etapowość ta daje bankom możliwość analizy i rozpoznania celowości wykorzystywania nowego kanału dystrybucji, kosztów z nim związanych, zainteresowania nim klientów, czy wreszcie poziomu bezpieczeństwa. Na każdym kolejnym etapie stosowany jest coraz wyższy, bardziej zaawansowany poziom zabezpieczeń.

2. Zabezpieczenia bankowości internetowej

2.1. Zabezpieczenia stosowane na pierwszym etapie rozwoju bankowości internetowej

Pierwszy etap rozwoju bankowości internetowej – prezentacja instytucji bankowej – polega na stworzeniu strony internetowej banku, stanowiącej jego elektroniczną wizytówkę. Faza ta charakteryzuje się zamieszczaniem w serwisie www podstawowych informacji dotyczących samego podmiotu (historia, akcjonariusze, struktura organizacyjna, władze, placówki itp.) oraz jego oferty. Niekiedy banki umożliwiają w ten sposób klientom zapoznanie się z regulaminami oferowanych produktów, a także z aktualnymi tabelami opłat i prowizji ich dotyczącymi czy z kursami walut.

Dla banku ten etap ewolucji wiąże się z niewielkim ryzykiem, często więc jest wykorzystywany do nauki – poznawania Internetu i klientów. Witryny internetowe są wizytówką poszczególnych instytucji bankowych w sieci, a ich wygląd jest jednym z czynników wpływających na decyzję o rozpoczęciu korzystania z usług danego banku za pośrednictwem Internetu. Użytkownik odwiedzający witrynę banku oczekuje od niej swobody poruszania się oraz aktualnej, łatwo dostępnej informacji. Bank zaś, jako właściciel serwisu www, musi te wymagania połączyć z dynamicznie zmieniającą się zawartością i wyglądem strony.

Jeśli chodzi o rodzaj zabezpieczeń, to na tym etapie banki po swojej stronie instalują tzw. *firewalls* (ściany ognia, zapory ogniowe), filtrujące wszystkie informacje przychodzące do banku. Jeśli urządzenie wykryje, że dane pochodzą z nieznanych lub nieuprawnionych źródeł, to nie przekazuje ich do wnętrza systemu. Zabezpieczenia te gwarantują, że wewnętrzna struktura sieci komputerowej pozostaje niewidoczna z zewnątrz. Zadanie to zazwyczaj wykonuje oddzielny komputer z odpowiednim oprogramowaniem, pośrednicząc w przepływie wszystkich informacji między instytucją i resztą świata [6, s. 33].

2.2. Zabezpieczenia stosowane na drugim etapie rozwoju bankowości internetowej

Na początku najważniejsza była sama obecność w sieci, nadająca instytucji bankowej wizerunek firmy nowoczesnej, wykorzystującej najbardziej zaawansowane technologie. Jednak z czasem serwisy internetowe banków przestały być narzędziem ich przewagi nad konkurencją, a stały się koniecznością [14, s. 34]. Wobec tego zaczęto je coraz bardziej rozbudowywać i lepiej dopasowywać do potrzeb użytkowników Internetu. Dołączano kolejne możliwości, takie jak chociażby wymiana informacji poprzez pocztę elektroniczną. Komunikacja e-mailowa stanowi namiastkę drugiego etapu wprowadzania Internetu do działalności banku, albowiem w odniesieniu do niej można już mówić o interakcji między bankiem i klientem. Użytkownik ma możliwość korzystania z wyszukiwarek, kalkulatorów pożyczek czy lokat, które pozwalają na obliczenie należnych mu odsetek. Klient za pośrednictwem Internetu może uzupełnić ankietę, dającą wyraz jego wymaganiom i oczekiwaniom wobec banku, czy złożyć wniosek, np. otwarcia rachunku oszczędnościowo-rozliczeniowego. Poza tym klient może skorzystać z porad bankowców, czy wreszcie zostaje mu udostępniony pasywny dostęp do własnego konta, tj. dający możliwość sprawdzania salda i historii rachunku.

Na drugim etapie rozwoju bankowości internetowej są stosowane oprócz *firewall* także inne zabezpieczenia, takie jak szyfrowana transmisja danych za pomocą protokołu SSL i uwierzytelnianie proste.

Przechodząc do krótkiej charakterystyki wyżej wymienionych sposobów zabezpieczeń, można powiedzieć, że pierwszy z nich ściśle wiąże się z kryptografią, tj. nauką wykorzystywaną pierwotnie do celów wojskowych, spokrewnioną z matematyką, a zajmującą się metodami szyfrowania i deszyfrowania wiadomości, danych itp. Polega to na transformowaniu informacji tak, aby stała się ona nieczytelna dla każdego z wyjątkiem zamierzonego odbiorcy, a następnie na przeprowadzeniu procesu odwrotnego, zmieniającego zakodowaną informację, ażeby możliwe było jej ponownie odczytanie przez adresata [8, s. 49].

W celu zapewnienia bezpieczeństwa informacji banki stosują różne metody szyfrowania. Najbardziej rozpowszechnioną z nich jest kryptografia oparta na klu-

czach symetrycznych. Ma ona wielowiekową praktykę, a zakłada, że istnieje jeden tajny kod (klucz), który służy zarówno do szyfrowania, jak i do rozszyfrowywania wiadomości. Podstawową zaletą kryptografii symetrycznej jest jej szybkość, wydajność oraz odporność na łamanie. O bezpieczeństwie systemu w głównej mierze decyduje jakość zastosowanego algorytmu oraz długość klucza używanego do szyfrowania transmisji. W praktyce polskich banków stosowane są 128-bitowe klucze wykorzystywane jednorazowo w danej sesji [19, s. 2]. Teoretycznie zabezpieczenia związane z tą metodą szyfrowania mogą być złamane, np. przez sprawdzanie każdej możliwej kombinacji znaków tworzących klucz. Osiągnięcie tego celu jest tylko kwestią czasu i nakładów, które musiałyby zostać poniesione. Dostępne w 2000 r. moce obliczeniowe komputerów umożliwiały złamanie klucza o długości 40 bitów w ciągu ośmiu godzin [9, s. 66]. Jednak już zwiększenie długości klucza o zaledwie 1 bit oznacza podwojenie nakładów (mocy obliczeniowej) koniecznych do rozszyfrowania wiadomości (tab. 1).

Tabela 1. Teoretyczne maksymalne czasy złamania kluczy klasy DES/RC-4

Liczba bitów klucza	Czas złamania kluczy klasy DES/RC-4
40	0,4 s /15 dni
56	7 godz. /2691,49 w roku
64	74 godz. 40 min. /689 021,57 w roku
128	157129203952300000 lat/ 127102046526100000000000000 lat

Źródło: [6, s. 33].

W polskich bankach, oferujących swoje usługi przez Internet, w celu zapewnienia bezpiecznej szyfrowanej komunikacji stosowany jest przeważnie protokół SSL (*Secure Sockets Layer*). To narzędzie, gwarantujące prywatność i autentyczność cyfrowej komunikacji, stworzyła firma Netscape Communications [10, s. 116]. Ważne jest, że korzystanie z niego praktycznie nie wymaga od użytkownika wykonywania żadnych manualnych czynności. Wszystkie bowiem operacje kodowania i dekodowania informacji odbywają się automatycznie. W trakcie nawiązywania połączenia między serwerem bankowym a komputerem klienta, ustalany jest algorytm szyfrowania, wymieniane są klucze oraz weryfikowana jest (np. z użyciem certyfikatów) autentyczność zarówno serwera, jak i klienta. Użytkownik bankowości elektronicznej może sprawdzić zastosowanie protokołu SSL w okienku adresu przeglądarki – adres URL zaczyna się wówczas od liter „https://" (zamiast zwykłego „http://"), a przeglądarka (np. Intemet Explorer) wyświetla informację następującej treści: „Za chwilę obejrzysz strony w bezpiecznym połączeniu. Informacje wymieniane z tą witryną nie są widoczne dla nikogo innego w sieci Web". Jednocześnie na pasku u dołu ekranu monitora pojawia się zamknięta kłódka, która symbolizuje bezpieczne połączenie. Kliknięcie na kłódkę umożliwia za-

poznanie się z informacjami o certyfikacie posiadanym przez serwer instytucji finansowej, której strony właśnie odwiedza internauta.

Kolejnym rodzajem zabezpieczeń systemów bankowości internetowej stosowanym przez banki przy pasywnym dostępie klienta do rachunku bankowego jest uwierzytelnianie proste. Służy ono identyfikacji stron transakcji. Jego zadaniem jest uniemożliwienie powstania sytuacji, w której jedna osoba „podszywałaby się" pod inną. Do najprostszych metod uwierzytelnień zalicza się identyfikatory i przyporządkowane im hasła. Składają się one z szeregu znaków. Dla podwyższenia bezpieczeństwa zaleca się stosowanie procedur komplikujących złamanie zabezpieczeń. Na przykład hasło powinno zawierać przynajmniej dwie cyfry, dwie litery, tak aby dowolny znak nie powtarzał się więcej niż trzy razy. Korzystna jest także jego okresowa zmiana. W razie parokrotnego błędnego wprowadzenia określonego ciągu znaków system blokuje dostęp do rachunku użytkownika, a ponowne jego odblokowanie odbywa się przeważnie alternatywną drogą kontaktu z bankiem. Weryfikacja klienta następuje po porównaniu hasła związanego z danym identyfikatorem, które on sam podał, z hasłem zapisanym w systemie bankowym. Jednak aby stosowanie tego rodzaju zabezpieczeń miało sens, ich transmisja powinna się odbywać w bezpiecznym (szyfrowanym) połączeniu, o którym była mowa powyżej.

2.3. Zabezpieczenia stosowane na trzecim etapie rozwoju bankowości internetowej

Na trzecim etapie rozwoju bankowości internetowej związanym z realizacją pełnego zakresu usług bankowych przez Internet, w literaturze niekiedy określanym jako „prawdziwa bankowość internetowa" [4, s. 183], występuje już pełna więź pomiędzy bankowym systemem zaplecza a stroną www. Typowy użytkownik tego rodzaju usług korzysta z nich głównie po to, aby dysponować bieżącą informacją o stanie swojego konta, jak również by móc dokonywać przelewów na inne rachunki bankowe (np. płatności za prąd, telefon) bez konieczności wizyt w oddziale. Stąd też te operacje stanowią trzon każdego z systemów bankowości internetowej. Obok przelewów jednorazowych banki oferują także zlecenia stałe, którymi można regulować powtarzające się okresowo płatności. Poza tym w części instytucji bankowych można przez Internet założyć lokatę bądź ją zlikwidować, wystąpić o kartę płatniczą oraz limit kredytowy na koncie. Decydując się na korzystanie z sieciowych rachunków, klient chce do maksimum ograniczyć wizyty w tradycyjnym oddziale. Jednak czasem musi zadać pytanie dotyczące swojego konta – gdy np. zamierza złożyć reklamację, chce dowiedzieć się, skąd wzięła się jakaś „tajemnicza" operacja, albo zależy mu na wyjaśnieniu, czy odsetki są rzeczywiście poprawnie naliczone. Wówczas przydatna okazuje się możliwość prowadzenia poufnej korespondencji [18, s. 3]. Pytań o konto nie można zadawać za pośrednic-

twem zwykłej poczty elektronicznej, gdyż bank musi mieć pewność, że list pochodzi od właściciela konta, a klientowi zależy, aby nikt obcy nie przeczytał korespondencji. Korespondencję wysłaną z wnętrza systemu bankowości internetowej instytucje finansowe traktują – w przeciwieństwie do zwykłego e-maila – jak list polecony.

Stosowany na tym etapie rozwoju bankowości internetowej rodzaj zabezpieczeń to – poza wyżej omówionymi – uwierzytelnianie złożone. Sprowadza się ono do haseł jednorazowych, które mogą być wydrukowane na specjalnej karcie TAN (skrót niemieckiego *TransAktion Nummer*) lub generowane przez token. Wśród metod uwierzytelniania złożonego znajdują się również takie, które wykorzystują podpis elektroniczny.

Token to urządzenie elektroniczne przypominające wyglądem breloczek lub kalkulator wielkości karty płatniczej, na którego ciekłokrystalicznym ekranie wyświetla się szereg znaków. Właśnie dzięki nim bank może być pewien, że z rachunku korzysta uprawniona osoba, ponieważ identyczny ciąg znaków występuje zarówno na tokenie klienta, jak i po stronie serwera banku. Każda operacja skutkująca zmianą salda konta bankowego jest potwierdzana wprowadzeniem aktualnego kodu widniejącego na tokenie. Generator haseł jednorazowych, np. Lukas Banku S.A., wyświetla również skalę czasu odmierzającą upływające sekundy, co informuje użytkownika, przez jaki czas ważne będzie jeszcze dane hasło, które zmienia się samoczynnie na nowe co 60 sekund. Niektóre z tego rodzaju urządzeń mają klawiaturę, która pozwala dodatkowo zabezpieczyć je PIN-em. W razie parokrotnego błędnego wprowadzenia kodu token się zablokuje. Próba zaś rozmontowania np. tokena ActiveCard Plus zakończy się wylaniem specjalnego płynu, który zniszczy znajdujący się w jego wnętrzu układ. Wspomniane urządzenie stosowane przez PKO BP SA używane jest tylko raz podczas danej sesji – przy logowaniu do systemu. Najpierw klient podaje identyfikator i hasło do konta. Po poprawnej weryfikacji system wyświetla 6-cyfrowe pytanie, po czym użytkownik włącza token, wystukując jego PIN. Za pomocą specjalnej funkcji wprowadza pytanie, na które urządzenie generuje kryptograficzną odpowiedź, złożoną z 6 znaków (cyfry i litery). Czas na przepisanie odpowiedzi tokena do przeglądarki jest niemal nieograniczony (kilka godzin). W razie pozytywnej autoryzacji następuje poprawne zalogowanie do systemu bankowego. Token, o którym mowa, wykorzystuje tzw. metodę *challenge-response*, czyli hasło-odzew [7, s. 40].

Niektóre banki rezygnują z zaawansowanych technik kryptograficznych, powierzając bezpieczeństwo pieniędzy klientów jedynie systemowi haseł. Wykorzystują do tego celu tzw. karty haseł jednorazowych – TAN, które przesyłają swoim klientom. Każde hasło z listy wykorzystywane jest do jednej potencjalnie niebezpiecznej operacji, np. polecenia przelewu, po czym traci ważność – do następnej operacji należy wykorzystać inne hasło. Po zużyciu wszystkich haseł klient zamawia kolejną ich listę.

Podstawę funkcjonowania podpisu elektronicznego stanowi tzw. system klucza publicznego *(Public Key Infrastructure)*, nie tylko zapewniający sprawdzenie tożsamości obu stron transakcji, ale także uniemożliwiający zaprzeczenie udziału w niej. Daje on uczestnikom pewność, iż przesyłane przez nich dane, dokumenty oraz oświadczenia woli dotrą do adresata w niezmienionej postaci, każda bowiem ich modyfikacja dokonana po złożeniu podpisu elektronicznego jest wykrywalna [17, s. 3].

Podpis elektroniczny opiera się na metodzie szyfrowania parą kluczy asymetrycznych. Polega to na tym, że każda ze stron ma dwa zależne od siebie i tworzące parę klucze. Jeden używany do szyfrowania wiadomości, który nazywa się kluczem publicznym. Określenie to pochodzi stąd, że musi go znać każdy, kto chce wysłać posiadaczowi klucza zaszyfrowaną wiadomość. Drugi zaś z nich to klucz prywatny. Ten z kolei służy do rozszyfrowywania danych i należy strzec go ze szczególną starannością, nie może bowiem poznać go nikt poza jego właścicielem [15, s. 9]. Wspomniana para kluczy znajduje się we wzajemnej zależności matematycznej – na podstawie klucza prywatnego łatwo oblicza się odpowiadający mu klucz publiczny. Natomiast odwrotna zależność, tj. „złamanie" klucza prywatnego na podstawie klucza publicznego, jest prawie niemożliwa do wykrycia. W najczęściej używanym do szyfrowania asymetrycznego algorytmie RSA (*Rivest-Shamir-Adleman* – skrót od nazwisk twórców) klucz prywatny składa się z dwóch dużych (rzędu 100 cyfr) liczb pierwszych, klucz publiczny zaś jest ich iloczynem. Metoda złamania szyfru, czyli odtworzenia klucza prywatnego, gdy ma się dany klucz publiczny, jest zatem teoretycznie oczywista: należy tę liczbę rozłożyć na czynniki pierwsze. Bezpieczeństwo szyfru płynie stąd, że w razie użycia wszystkich znanych obecnie metod matematycznych operacja rozkładu tak dużej liczby na czynniki trwa niezwykle długo. Algorytm szyfrowania z kluczem publicznym skonstruowany jest tak, że to, co zostanie zaszyfrowane kluczem publicznym, może być odszyfrowane jedynie kluczem prywatnym z tej samej pary. Działa to jednak również w odwrotną stronę: to, co zostanie zaszyfrowane kluczem prywatnym, może być odszyfrowane przez każdego, kto zna klucz publiczny. Oczywiście taki szyfr, który każdy może odczytać, jest zupełnie nieskuteczny jako szyfr, ale sprawdza się znakomicie jako podpis elektroniczny [3, s. 62].

W praktyce przy tworzeniu podpisu elektronicznego szyfrowaniu nie podlega cała wiadomość, lecz jej skrót kryptograficzny – kilkunasto- bądź kilkudziesięciobajtowa wartość, obliczona na podstawie treści wiadomości za pomocą tzw. funkcji mieszającej *(hash function)*. Funkcje takie mają tę prawidłowość, że niemożliwe jest skonstruowanie dwóch wiadomości, które dawałyby identyczny wynik funkcji mieszającej. Stąd najdrobniejsza nawet zmiana w treści dokumentu daje inną wartość skrótu, a zatem inny podpis elektroniczny [15, s. 20]. Właściwość ta zapewnia zatem weryfikację integralności.

3. Zakończenie

Każdy bank internetowy w swoich materiałach reklamowych zapewnia, że dzięki stosowaniu najnowocześniejszych technologii kryptograficznych pieniądze klientów są całkowicie bezpieczne. Niestety w przypadku niektórych instytucji bankowych nie jest to do końca prawdą. Taki wniosek można wysnuć, przyglądając się analizom opracowanym przez miesięcznik Chip, dotyczącym zabezpieczeń polskich banków internetowych [2, s. 146]. Autorzy zestawili tam w formie tabelarycznej informacje dotyczące bezpieczeństwa bankowych kont internetowych. Wzięto pod uwagę takie czynniki, jak liczba i długość haseł, rodzaj użytych technik kryptograficznych lub programistycznych, odporność na oprogramowanie szpiegujące, przechwytywanie haseł itp. Spośród opisanych systemów najsłabiej zabezpieczony okazał się system Citibanku. Opiera on bowiem swoje bezpieczeństwo jedynie na uwierzytelnianiu prostym. Metody uwierzytelniania użytkowników Citibank Online sprowadzają się do podania numeru karty i tzw. i-PIN-u. Wykorzystywane hasła dostępowe łatwo można podsłuchać czy wykraść zdalnie z komputera, stąd też nie powinno dziwić to, iż wspomniana instytucja bankowa jest ulubionym celem polskich i zagranicznych hakerów. Ponadto Citibank wielokrotnie pojawił się na liście najczęściej atakowanych instytucji. Spis ten zamieszczono na stronie organizacji Anti-Phishing Working Group (http://www.antiphishing.org), powołanej do walki z opisanymi przestępstwami.

Same hasła dostępowe to zbyt skromne zabezpieczenie; dopiero posługiwanie się jakimś elementem fizycznie powierzonym klientowi przez bank (listą haseł jednorazowych lub tokenem) ogranicza możliwość wirtualnej kradzieży. Karty TAN są stosowane m.in. w systemach Inteligo – PKO BP SA, mBanku – BRE Banku SA czy Pekao24. Tokeny zaś służą do zabezpieczania internetowych rachunków bankowych klienta, m.in. w Lukas Banku SA, Volkswagen Banku SA czy Banku Zachodnim WBK SA. Niewiele instytucji bankowych zdecydowało się na używanie podpisu elektronicznego. Rozwiązanie to stosują np. Bank Przemysłowo-Handlowy PBK SA, ING Bank Śląski SA oraz Fortis Bank Polska SA. Ostatnia z wymienionych instytucji od października 2004 r. udostępnia swoim klientom możliwość przechowywania ich klucza prywatnego na karcie chipowej, z której haker nie może go skopiować [2, s. 146]. To znacznie zwiększa bezpieczeństwo środków pieniężnych zgromadzonych na internetowym rachunku bankowym. Podpis elektroniczny jako jeden z rodzajów zabezpieczeń stosowanych w bankowości internetowej stanie się zapewne bardziej popularny po 2006 r., kiedy to zgodnie z zapisami ustawy o podpisie elektronicznym wszystkie organy administracji publicznej muszą być gotowe do przyjmowania drogą elektroniczną wszelkich pism, które obecnie składa się pisemnie oraz do odpowiadania na nie tą samą drogą [1, s. 6]. Wszystkie te dokumenty będą opatrzone kwalifikowanym podpisem elektronicznym.

Wszystkie te dokumenty będą opatrzone kwalifikowanym podpisem elektronicznym.

Literatura

[1] Biskupski J., *Tylko banki mogą spowodować przyspieszenie*, „Gazeta Prawna" 2003 nr 198.
[2] Borowski A., *Niepewne jak w banku*, „Chip" 2004 nr 12.
[3] Cwynar A., *Zabezpieczone podpisem*, „Bank" 2003 nr 9.
[4] Dziuba D. T., *Systemy informatyczne w obsłudze banków detalicznych*, Wydawnictwo UW, Warszawa 2002.
[5] E-banki (nie)bezpieczne? Raporty. http://e-biznes.interia.pl/rap/ (30.09.2004).
[6] Gogołek W., *Bezpieczeństwo sieci – Obrona, cz. II*, „Przegląd Techniczny" 1999 nr 1.
[7] Koniakowski J., *Elektroniczna bankowość po polsku*, „Internet" 2000 nr 4.
[8] Kosterna U., Pszczółka I., *Integracja systemów informatycznych dla potrzeb e-biznesu*, „Bank" 2000 nr 11.
[9] Łysakowski P., *Elektroniczne usługi finansowe*, „Bank" 2000 nr 7.
[10] Nowakowski M., *Protokół SSL zabezpieczenie internetowej transmisji danych – perspektywy rozwoju*, „Biuletyn Bankowy" 1999 nr 11.
[11] *Pierwszy wirtualny bank w Polsce*, „Biuletyn Bankowy" 1998 nr 11.
[12] Pilawski B., *Bankowość elektroniczna – zagrożenia, ograniczenia i bariery rozwoju*, [w]: *Zastosowania rozwiązań informatycznych w bankowości*, Prace Naukowe AE nr 872, AE,Wrocław 2000.
[13] Polasik M., *Boimy się e-banków*, VII Forum Bankowości Elektronicznej. http://internet.interia.pl/ (01.05.2004).
[14] Quirchmayr G., *Some effects of internet banking*, [w:] *Zastosowania rozwiązań informatycznych w bankowości*, Prace Naukowe AE nr 828, AE, Wrocław 1999.
[15] Rafa J., *e-podpis i co dalej?*, „Internet" 2002 nr 1.
[16] Ryznar Z., *Co umie haker?*, „Gazeta Bankowa" 2002 nr 16.
[17] Sitnicki I., Srebrny M., *Nie taki diabeł straszny, jak go malują*, „Rzeczpospolita" 2001 nr 33, dodatek „Prawo co dnia".
[18] Stankiewicz P., *Bank w domowym komputerze*, „Rzeczpospolita" 2000 nr 110, dodatek „Moje Pieniądze".
[19] Stankiewicz P., *Wirusy, włamywacze i oszuści*, „Rzeczpospolita" 2002 nr 136, dodatek „Moje Pieniądze".

INTERNET BANKING SAFETY

Summary

Internet banking appeared in Poland six years ago. Since then the number of Internet bank accounts has been increasing dynamically. At the end of June 2004 there were already 2,7 million of them. The number of Internet banking users would be even bigger if not the reported lack of the feeling of safety while communicating with the bank by means of www. site. Clients are afraid that the

information on their bank accounts and the data referring to performed operations may be broken into or modified by criminals. In order to prevent this banks use different types of safety measures related to the scope of their using the Internet as banking services distribution channel. Among them there are: so called firewalls, data transmission coding by means of SSL protocol, simple and complex authorization. The letter is carried out by means of single use pass words printed on a TAN card or generated by a token. Among the methods of complex authorization there are also these which use an electronic signature.