ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 797 STUDIA INFORMATICA NR 33 2013

Agnieszka Zalewska-Bochenko*
Uniwersytet w Białymstoku

ZABEZPIECZENIE BANKOWYCH USŁUG INTERNETOWYCH W POLSCE

Streszczenie

Banki zdają sobie sprawę z faktu, iż tradycyjna forma komunikowania się z klientami nie zaspokaja wszystkich deklarowanych potrzeb, a często jest wręcz niewygodna. Naturalną konsekwencją tego są więc coraz silniejsze więzi sektora bankowego ze środowiskiem informatycznym, pozwalające na skuteczne pokonywanie bariery czasu i przestrzeni, których jedną z podstawowych reguł jest odpowiedni poziom ochrony danych. Obecnie zatem konieczne stało się wypracowanie nowych sposobów zabezpieczania transakcji biznesowych, dokonywanych w dużej mierze drogą elektroniczną, przed potencjalnymi nadużyciami. Bez zagwarantowania właściwego poziomu bezpieczeństwa ich nowo powstałe odmiany nie mają żadnych szans na upowszechnienie, czy w ogóle na wdrożenie. Jednocześnie, z racji tego, że metody zabezpieczeń stale ewoluują bądź też są zastępowane nowszymi, trudno mówić, że są sprawdzone (Węsierska E., 2004, s. 66).

Słowa kluczowe: bezpieczeństwo, zagrożenie, usługi internetowe

Wprowadzenie

Zagadnienia bezpieczeństwa transakcji elektronicznych są podstawowym czynnikiem warunkującym rozwój usług bankowości internetowej. Ogromnym wyzwaniem dla banku jest pokonanie tej bariery rozwoju, określanej mianem bariery bezpieczeństwa. Wiąże się to z koniecznością inwestowania w odpowiednie technologie i zabezpieczenia systemu bankowego przed niepowołanym dostępem osób trzecich.

Transakcje realizowane za pośrednictwem Internetu kosztują mniej i są bardziej dostępne, jednak są też źródłem istotnych zagrożeń. Globalny charakter sieci

* agnieszkazal@poczta.onet.pl

sprawia bowiem, że wymiana informacji pozbawiona jest kontroli nad drogą przesyłania. Istnieje więc techniczna możliwość przechwycenia informacji na drodze komunikacyjnej między bankiem a klientem. Sieć Internetu, do której jest podłączony zarówno system informatyczny banku, jak i klient, jest narażona na ataki „sieciowych włamywaczy". Mogą oni zmieniać konfigurację systemu stosowanego przez bank, ingerować w transakcje, a nawet zmieniać stany kont. Bank działający w Internecie musi zatem nie tylko zadbać o dostarczenie odpowiednich technologii zabezpieczających transakcje, ale również przekonać do tego swoich klientów.

Niestety ignorancja większości społeczeństwa w kwestii bezpieczeństwa usług internetowych jest jednym z powodów ataków cyberprzestepców. Dodatkowo, w związku z coraz lepszymi metodami zabezpieczeń stosowanymi przez banki, okazuje się, że to klient jest najbardziej narażony na takie ataki. Są klienci, którzy uważają, iż kwestia bezpieczeństwa spoczywa na banku i dość nieuważne korzystają z bankowości internetowej, wchodząc na podejrzane strony, instalując nieznane programy, czy nie instalując systemów antywirusowych czy firewalli. Jest również grupa klientów, która w ogóle nie ma zaufania do bankowości internetowej i nie korzysta z jej udogodnień, a najczęstszym tego powodem, jest obawa przed włamaniem na konto bankowe, kradzieżą loginu i hasła, fałszywymi stronami banku, wirusami, podglądaniem konta przez innych. Banki powinny więc nieustająco walczyć z tymi zagrożeniami, ponieważ dla większości klientów są one barierą nie do pokonania, uniemożliwiającą korzystanie z tego typu usług.

Celem artykułu jest próba scharakteryzowania niebezpieczeństw, na jakie mogą być narażeni klienci korzystający z usług bankowości internetowej oraz sposobów zabezpieczeń stosowanych przez banki w celu przeciwdziałania owym zagrożeniom.

1. Zagrożenia bankowych usług internetowych

Bezpieczne świadczenie internetowych usług bankowych wymusza tworzenie sprawnych systemów zabezpieczających przed destrukcją systemów informatycznych i kradzieżą przez osoby nieupoważnione wartości posiadanych przez klienta banku. Bank musi wprowadzić takie mechanizmy ochrony bankowych systemów komputerowych, które zabezpieczają przed (Bogacka-Kisiel red., 2000, s. 608):

– sabotażem i zagrożeniami nieumyślnymi,
– infiltracją czynną,
– infiltracją bierną.

Klęski żywiołowe, pożary, awarie energetyczne, wirusy i robaki komputerowe, a także konie trojańskie należą do zagrożeń nieumyślnych lub sabotażu, który charakteryzuje się tym, że nie przynosi sprawcom materialnego czy też informatycznego zysku. Infiltracja zaś to „działania osób nieupoważnionych mające na celu przeniknięcie do poszczególnych elementów systemu informatycznego lub sieci komunikacyjnej z zamiarem zdobycia informacji" (Węsierska E., 2004, s. 135). Zagrożenie to może być bierne lub czynne, a sprawca dąży tu do osiągnięcia konkretnego zysku. Do pierwszej kategorii zaliczamy: łamanie zabezpieczeń, kopiowanie zbiorów niezabezpieczonych, podszywanie się pod uprawnionego użytkownika systemu, czyli wszelkie kroki mające na celu uzyskanie dostępu do systemu informatycznego i ujawnienie informacji w nieuprawiony sposób. Natomiast do drugiej kategorii, polegającej na śledzeniu informacji w określonym miejscu jej obiegu, zaliczamy: „przechwytywanie elektromagnetyczne, polegające na uzyskaniu dostępu bądź do połączeń między komputerem a terminalami, bądź do kierunkowej emisji promieniowania, dołączenie się do linii transmisji danych w sieciach telekomunikacyjnych lub przechwytywanie sygnałów przekazywanych drogą radiową, podsłuchiwanie w sieciach komputerowych, badanie i kopiowanie zbiorów niezabezpieczonych, analiza makulatury lub pozostałości po magnetycznych nośnikach informacji i stosowanie ukrytych nadajników" (Bogacka-Kisiel red., 2000, s. 608).

Mając na uwadze powyższy podział zagrożeń, możemy wyłonić specyficzne grupy przestępstw, które są szczególnie związane z bezpieczeństwem transakcji elektronicznych. Są to (Wawrzyniak D., 2005, s. 66):

1. *Hacking* komputerowy, zdefiniowany jako nieuprawnione wejście do systemu komputerowego przez naruszenie zastosowanych zabezpieczeń.
2. Podsłuch komputerowy, czyli nieuprawnione przechwycenie informacji możliwe dzięki najnowocześniejszym urządzeniom technicznym.
3. Bezprawne niszczenie informacji, czyli usuwanie zmian bądź utrudnianie osobie uprawnionej zapoznania z informacją.
4. Sabotaż komputerowy, czyli zakłócenie lub paraliż funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli.
5. Oszustwo komputerowe, przestępstwo polegające na osiągnięciu korzyści majątkowej lub wyrządzeniu innej szkody przez wpływ na automatyczne przetwarzanie, gromadzenie albo przesyłanie informacji.
6. Fałszerstwo komputerowe, polegające na przerabianiu lub podrabianiu dokumentów w formie zapisu elektromagnetycznego przez wyspecjalizowane urządzenia.

7. *Phishing*[1] polegający na oszukańczym pozyskiwaniu poufnej informacji osobistej, jak np. hasła, przez udawanie osoby godnej zaufania, której te informacje są pilnie potrzebne (Grobicki, 2005, s. 63).

W. Chmielarz i T. Koźliński wymieniają w swoich opracowaniach następujące techniki włamań, jak (Chmielarz, 2005, s.107–108; Koźliński, 2004, s. 87–88):
- łamanie haseł dostępu,
- nasłuch sieciowy,
- oszukiwanie zabezpieczeń,
- obejście lub zneutralizowanie istniejących zabezpieczeń,
- rejestracja promieniowania elektromagnetycznego,
- przechwytywanie otwartych połączeń sieciowych,
- blokowanie usług,
- wirusy komputerowe,
- luki bezpieczeństwa w przeglądarkach internetowych,
- problemy z bezpiecznym transportem danych,
- zagrożenia płynące z niedoskonałości systemów operacyjnych,
- *spoofing*, polegający na zbudowaniu serwisu WWW, np. przypominającego wizualnie rzeczywiste serwisy bankowe lub maklerskie,
- skopiowanie historii rachunku bankowego klienta po wcześniejszym wyłudzeniu haseł dostępu i prezentowanie jej na fałszywym serwisie,
- podszywanie się pod personalia innej osoby,
- oprogramowanie przechwytujące hasła na podstawie śledzenia i zapamiętywania sekwencji wpisywanych liter i cyfr,
- nieprawidłowe skonfigurowanie przeglądarki internetowej, co może skutkować zezwoleniem na zainstalowanie dowolnych skryptów i kontrolek Active X, zmniejszających bezpieczeństwo korzystania z internetowego banku.

2. Środki zabezpieczenia bankowych usług internetowych

Problematyka bezpieczeństwa zasobów informacji w e-bankingu jest niezwykle szeroka i ma charakter interdyscyplinarny. Obejmuje aspekty techniczne, organizacyjne i prawne. Wszelkie problemy muszą być rozwiązywane przez zespoły specjalistów z tych obszarów. Systemy bankowości internetowej oferowane przez banki muszą zapewnić klientowi bezpieczeństwo jego informacji podczas transmisji

[1] *Phishing* – słowo to powstało w latach dziewięćdziesiątych i wywodzi się z angielskiej zbitki wyrazów *password harvesting fishing*.

danych w systemie oraz ochronę przed nieautoryzowanym dostępem lub próbą manipulacji przez osoby niepowołane. W tym celu stosuje się specjalne mechanizmy bezpieczeństwa, obejmujące wszystkie czynności operacyjne w systemie (Michalski, 2002, s. 134).

Aby zapewnić odpowiedni poziom bezpieczeństwa systemów bankowych, używa się licznych narzędzi informatycznych, wśród których można wyróżnić (Bilski T., 2000, s. 394–407):

1. Analizatory wersji oprogramowania i pakietów naprawczych – oprogramowanie, które na podstawie wprowadzonych przez użytkownika informacji o numerach wersji i zainstalowanych pakietach naprawczych generuje listę potencjalnych zagrożeń i listę potencjalnych pakietów naprawczych.
2. Skanery zabezpieczeń – oprogramowanie skanujące potencjalne zagrożenia systemu i prezentujące wyniki analizy.
3. Analizatory bezpieczeństwa haseł użytkowników – oprogramowanie wyszukujące łatwe sposoby odgadnięcia haseł i publikujące listy haseł niedozwolonych.
4. Pułapki i przynęty – oprogramowanie służące do zbierania informacji o metodach działania intruzów (śledzenie, udostępnianie, wnioski).
5. Narzędzia do wykrywania nadużyć i włamań – oprogramowanie służące do wykrywania naruszeń integralności plików, systemy wykrywania włamań, oprogramowanie do wykrywania nadużyć uprawnionych użytkowników, zewnętrzne monitorowanie systemu.
6. Ochrona przed błędami oprogramowania – eliminacja błędów przez instalowanie nowszych wersji oprogramowania i pakietów naprawczych, przechwytywanie wywołań.

Bezpieczeństwo w dokonywaniu operacji bankowych to nie tylko uniemożliwienie dostępu do kont osobie niebędącej jego właścicielem lub pełnomocnikiem, chociaż należy podkreślić, że jest to sprawa zasadnicza. Chodzi również o zachowanie tajemnicy bankowej, czy prawidłowości przesyłanych drogą elektroniczną danych. Rolą stosowanego systemu zabezpieczeń jest wypełnienie następujących zadań (Jurkowski, 2001, s. 18):

1. Uniemożliwienie dokonywania transakcji na rachunkach przez osoby niepowołane.
2. Uniemożliwienie osobom nieuprawnionym podglądania transakcji, kont oraz dostępu do innych danych podlegających prawnej ochronie lub tajemnicy bankowej.
3. Chronienie składanych zleceń przed zniekształceniem w trakcie transmisji.
4. Uniemożliwienie wyparcia się przez klienta dokonanych transakcji.

M. Samcik uszeregował najpopularniejsze zabezpieczenia od najmniej bezpiecznych do najskuteczniejszych. Według autora klasyfikacja ta jest następująca (Samcik, 2006):

1. Login – podstawowy identyfikator klienta łączącego się zdalnie z bankiem.
2. Hasło stałe – łącząc się z bankiem, podajemy je w całości, narażając się na jego podpatrzenie przez hakera.
3. Hasło maskowane – podajemy tylko niektóre cyfry z hasła. Haker ma utrudnione zadanie, bo za jednym razem nie pozna całego hasła.
4. Hasło jednorazowe z listy – bank przesyła na adres domowy klienta zalakowaną kartę kodów. Podajemy je, definiując lub wykonując przelewy. Dla utrudnienia życia podglądaczom hasła mogą być ukryte przez zdrapki lub bank może prosić o ich podanie losowo, a nie po kolei.
5. Hasło SMS – na zarejestrowany w banku numer telefonu bank wysyła jednorazowe hasło, którym zatwierdzamy transakcję. Bardziej zaawansowana i bezpieczniejsza forma haseł jednorazowych.
6. Klucz prywatny – specjalny plik komputerowy zainstalowany na serwerze banku lub w komputerze użytkownika. Przed wykonaniem przelewu trzeba wskazać jego położenie.
6. Token – miniaturowy generator kodów. Aby go uruchomić potrzebujemy specjalnego hasła, potem na wyświetlaczu pokazuje się ciąg cyfr, które trzeba wpisać przed wykonaniem przelewu. Hasło zmienia się co 30 sekund. Haker, nawet gdyby je przechwycił, nie zdąży zrobić z niego użytku.

Zdecydowanie najlepsze efekty przynosi zastosowanie rozwiązań hybrydowych, łączących w sobie różne metody uwierzytelniania. Kontrola dostępu do systemów bankowości elektronicznej opiera się przede wszystkim na tym, co użytkownik zna i co użytkownik ma, a więc na hasłach oraz dodatkowych atrybutach jednoznacznie identyfikujących użytkownika, takich jak tokeny.

Główna odpowiedzialność za bezpieczeństwo transakcji spoczywa na banku, ponieważ nieprawidłowości, jakie mogą tu wystąpić, narażają wielu jego klientów. Potwierdzają to wysokie straty spowodowane w bankach oszustwami komputerowymi. Można zatem stwierdzić, że właściwie eksploatowany system zabezpieczeń spełnia m.in. następujące zadania (Grzywacz, 2004, s. 120–121):

1. Zabezpieczenie przed naruszeniem tajności danych, przez co uniemożliwia osobom nieupoważnionym „podglądanie" transakcji, kont oraz dostęp do innych danych podlegających prawnej ochronie lub tajemnicy bankowej.
2. Uniemożliwia dokonanie transakcji na rachunkach przez osoby niepowołane.

3. Ochrania składane zlecenia przed zniekształceniem w trakcie transakcji, gwarantuje zatem integralność danych przesyłanych siecią, co oznacza, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
4. Uniemożliwia wyparcie się przez klienta dokonanych transakcji, a także zapewnia autentyczność podmiotów, co oznacza chociażby możliwość weryfikacji uprawnień klienta do korzystania z konta.
5. Gwarantuje dostępność autoryzowanych podmiotów biorących bezpośredni lub pośredni udział w transakcji elektronicznej w danym czasie.
6. Umożliwia kontrolę działań użytkowników w systemie.
7. Zabezpiecza przed zablokowaniem usługi, polegającym na zaburzeniu toku pracy użytkownika, np. przez wirusy komputerowe.

Bankowość internetowa widziana przez pryzmat bezpieczeństwa jest w pewnym sensie specyficzna. Z jednej strony bank udostępnia swoje zasoby informatyczne, z drugiej strony klient też musi skorzystać z połączenia internetowego, które może nieść ze sobą pewne niebezpieczeństwa. Takie otwarcie systemów na zewnątrz stwarza możliwość ataku hakerów, którzy mogą próbować włamać się do sieci. Jednym z zabezpieczeń przed tego typu atakami jest ściana ogniowa. Technologia ta zabezpiecza przed niedozwolonymi sposobami komunikacji z serwerem, co w praktyce oznacza niedopuszczenie przepływu danych na innych portach niż dozwolone. Z wielu opracowań można dowiedzieć się o różnych rodzajach zabezpieczeń stosowanych w bankowości internetowej. W większości przeważają jednak cztery główne. Są to (Wroński, 2004, s. 58–59; Jurkowski, 2001, s. 19):

– szyfrowanie transmisji danych,
– proste uwierzytelnianie, np. login, hasło,
– silne uwierzytelnianie, np. token,
– podpis elektroniczny.

Najczęściej używaną technologią zabezpieczeń, ze względu na jej relatywną prostotę i bezpieczeństwo, jest szyfrowanie oparte na rozwiązaniach protokołu szyfrującego SSL[2]. Szyfrowanie jest to takie przekształcenie informacji, które sprawia, że treść przekazywanej informacji jest niezrozumiała dla przypadkowe-

[2] SSL – (ang. Secure Sockets Layer) jest protokołem kryptograficznym opracowanym przez firmę Netscape Communications, zapewniającym bezpieczny kanał komunikacyjny między klientem a serwerem. Jest wykorzystywany do przesyłania zaszyfrowanych informacji za pośrednictwem Internetu. Obsługuje go większość popularnych przeglądarek internetowych, jak i serwerów WWW. Został powszechnie przyjęty jako standard szyfrowania na stronach internetowych.

go obserwatora, a po ponownym przekształceniu za pomocą specjalnego algorytmu przez użytkownika uprawnionego przybierająca swoją pierwotną postać (Chmielarz, 2005, s. 181). Z kryptograficznego punktu widzenia SSL jest hybrydą, to znaczy do szyfrowania używa zarówno algorytmów symetrycznych, jak i niesymetrycznych. Szyfrowanie danych przekazywanych pomiędzy użytkownikiem internetowego banku a bankiem jest oparte na dwóch elementach: algorytmie i kluczu. W algorytmach symetrycznych podczas szyfrowania do odszyfrowania używa się identycznego klucza. Klucz ten zostaje przekazany obydwu stronom transakcji za pośrednictwem odpowiednio zabezpieczonego kanału informacyjnego (Grzywacz, 2004, s. 124–125). Główną wadą tej metody jest konieczność uzgodnienia przez nadawcę i odbiorcę tajnego klucza w sposób dyskretny i przekazanie go sobie w sposób, który nadal będzie gwarantował zachowanie tajności.

Szyfrowanie asymetryczne polega na użyciu dwóch kluczy, prywatnego i publicznego. W tym przypadku klucz prywatny jest tajny i użytkownik nie może go udostępniać komukolwiek. Korzystając z szyfrowania asymetrycznego, wiadomość koduje się kluczem publicznym banku, co gwarantuje, że może być ona odczytana tyko przez bank, który posiada odpowiedni klucz prywatny. Natomiast szyfrowanie wiadomości do banku kluczem prywatnym klienta powoduje, że każdy może odczytać tę wiadomość. Dlatego klucz prywatny klienta wykorzystuje się do podpisania cyfrowej wiadomości szyfrowanej kluczem publicznym banku (Koźliński, 2004, s. 80).

Podstawowymi zabezpieczeniami stosowanymi w bankowości internetowej są stały login i stałe lub maskowane hasło (to oznacza, że wymagane jest podanie tylko wybranych znaków). Ich znajomość jest niezbędna, by uzyskać dostęp do rachunku choćby w trybie pasywnym, a więc np. móc podejrzeć stan konta i historię wykonanych operacji. Do wykonania potencjalnie ryzykownych transakcji, wiążących się z wytransferowaniem pieniędzy z konta, potrzebne jest jeszcze jedno potwierdzenie, że osoba wydająca dyspozycję jest do tego uprawniona. Tym dodatkowym uwierzytelnieniem najczęściej jest jednorazowe hasło, wygenerowane na jeden z kilku proponowanych przez banki sposobów. (Cerega, 2012).

Najbardziej popularnym rozwiązaniem są jednorazowe hasła SMS wysyłane na zarejestrowany przez klienta w banku numer telefonu komórkowego. Takie rozwiązanie bardzo ogranicza prawdopodobieństwo, że z pieniędzy zgromadzonych na rachunku skorzysta osoba nieuprawniona. Dodatkowo jednorazowe hasło

SMS jest generowane dopiero w momencie wykonywania transakcji, dlatego jest z nią ściśle powiązane. Gdyby osoba trzecia przechwyciła dane wymieniane między użytkownikiem a bankiem i próbowała je zmodyfikować, np. zmieniając dane beneficjenta przelewu, hasło przestanie być skuteczne. Zaletą tego rozwiązania jest też prostota, duża dostępność i niewielkie koszty (Cerega, 2012).

Najmniej zaawansowanym technologicznie rozwiązaniem są mające fizyczną postać (plastikowej karty lub papierowego wydruku) listy haseł jednorazowych. Bank z góry przygotowuje i wysyła klientowi listę np. 50 kolejno ponumerowanych haseł. W momencie, gdy użytkownik systemu bankowości internetowej składa potencjalnie ryzykowną dyspozycję, musi ją zatwierdzić kodem o wskazanym numerze. Użytkownicy bankowości internetowej mogą się też posługiwać dwoma rodzajami urządzeń generujących hasła jednorazowe. Są to tokeny sprzętowe, czyli niewielkie urządzenia elektroniczne z wyświetlaczem, na którym prezentowane jest hasło, oraz działające w podobny sposób aplikacje na telefon komórkowy, zwane tokenami GSM (Cerega, 2012).

Tokeny należą do tych zabezpieczeń, które zapewniają silne uwierzytelnianie ich posiadaczom. Działanie tokenu polega na generowaniu specjalnych, unikatowych ciągów cyfr, które następnie klient banku wprowadza do komputera. Sam proces generowania ciągu opiera się na kluczu prywatnym klienta, koncie, bieżącym czasie lub na innym ciągu cyfr (Jurkowski, 2001, s. 28). Używany do tego algorytm szyfrujący z reguły stanowi tajemnicę działania tokena. Weryfikacja ciągu cyfr wygenerowanych przez token dokonywana jest przez system komputerowy banku, który zna klucze tokenów oraz ich algorytm.

Jedną z ciekawszych metod ochrony jest podpis elektroniczny. Dzięki swojej niezaprzeczalności w założeniu ma umożliwić jednoznaczną identyfikację użytkownika systemu bankowości internetowej (Hołownia, 2007, s. 22). Poza tym podpis elektroniczny musi spełniać te same warunki co podpis odręczny, tzn. powinien być trudny lub niemożliwy do podrobienia, umożliwiać weryfikację i trwale łączyć się z dokumentem. Za podpis elektroniczny w Polsce uważa się „przekształcenie kryptograficzne danych umożliwiające odbiorcy danych sprawdzenie autentyczności, integralności danych oraz zapewniające nadawcy ochronę przed sfałszowaniem danych przez odbiorcę" (Wroński, 2004, s. 59). Podpis elektroniczny gwarantuje uwierzytelnianie transakcji i weryfikuje na odległość tożsamość osoby logującej się do systemu. Zapewnia bezpieczeństwo – zarówno bankowi, jak i klientowi – jakiego nie dają rozwiązania bazujące na hasłach, kodach jednorazowych, tokenach. Przechwycenie

przez niepowołaną osobę podpisanej transakcji co najwyżej grozi tym, że nie dotrze ona do banku. Haker nie może jej wykorzystać, gdyż jakakolwiek jej modyfikacja lub też przyklejenie oryginalnego podpisu do podstawionej transakcji zostanie wykryte w momencie weryfikacji przez bank. Co więcej, zastosowanie bezpiecznego podpisu elektronicznego i certyfikatów kwalifikowanych przez klienta daje również bezpieczeństwo prawne bankowości. Zgodnie z przepisami ustawy o podpisie elektronicznym klient nie może wyprzeć się takiej transakcji, chyba że wcześniej unieważnił swój certyfikat (Włodarczyk, 2007, s. 49).

Przyjęta w 2001 roku ustawa[3] o podpisie elektronicznym, która weszła w życie w 2002 roku, stwarza podstawy do bezpiecznego zawierania transakcji w Internecie. Zawiera regulacje zrównujące w skutkach prawnych tzw. bezpieczny podpis elektroniczny z podpisem własnoręcznym. Jednym z jej elementów było także stworzenie ram prawnych działalności podmiotów certyfikujących, których zadaniem jest potwierdzanie tożsamości kontrahentów korzystających z podpisu elektronicznego. Swojego rodzaju wstępem do używania podpisu elektronicznego było zrównanie dokumentu papierowego z elektronicznym na podstawie Prawa bankowego z 29.08.1997 roku (Hanusik i Machulik, 2004, s. 59).

Banki proponujące więcej niż jeden sposób zabezpieczania transakcji zwykle deklarują, że jest to stan docelowy i chcą pozostawić klientom wybór metody, którą ci uważają za najwygodniejszą. I tak np. Deutsche Bank zakłada, że klienci będą głównie korzystać z haseł SMS, ale pozostawia w użyciu tradycyjną kartę z hasłami. Kredyt Bank i Eurobank rekomendują używanie tokena GSM jako najbezpieczniejszego i najwygodniejszego rozwiązania, ale również nie zamierzają rezygnować z jego alternatyw. Z kolei Credit Agricole ze względu na wygodę rekomenduje posługiwanie się hasłami SMS, ale zapewnia, że równie bezpieczna jest druga metoda, czyli używanie tokena. Także mBank zamierza pozostawić dwie metody (papierowe listy haseł i kody SMS), jednak zaznacza, że klienci, którzy chcą korzystać z bankowości mobilnej, muszą się zdecydować na to drugie rozwiązanie. Dodatkowo za wydanie każdej papierowej listy trzeba zapłacić, podczas gdy korzystanie z kodów SMS jest darmowe. Podobnie wygląda cennik Banku BPS. Klienci mogą korzystać z kodów SMS i haseł z tradycyjnej listy, bank zamierza pozostawić oba te rozwiązania, jednak z uwagi na koszty dystrybucji korzystanie z tradycyjnych list jest płatne, a z haseł SMS – darmowe (Cerega, 2012).

[3] W wyniku wcześniejszych działań ustawa zaczęła obowiązywać od 16 sierpnia 2006 r.

Tabela 1

Metody autoryzacji przelewów internetowych

Bank	Dostępne rozwiązania
Bank Pocztowy	lista kodów (bezpłatnie), hasła SMS (bezpłatnie)
BGŻ	hasła SMS (bezpłatnie); dodatkowo dla starych klientów lista kodów (bezpłatnie), token (30 zł)
BNP Paribas	hasła SMS (bezpłatnie), podpis elektroniczny (20 zł za wydanie nośnika)
BPH	hasła SMS oraz podpis elektroniczny stosowane łącznie (0–0,35 zł za hasło)
BPS	lista kodów (5 zł), hasła SMS (bezpłatnie)
BZ WBK	hasła SMS (0–0,2 zł za hasło)
Citi Handlowy	hasła SMS (bezpłatnie), hasła do odsłuchiwania przez IVR (bezpłatnie)
Credit Agricole	hasła SMS (bezpłatnie), token (0 lub 5 zł/mies.)
Deutsche Bank	lista kodów(bezpłatnie), hasła SMS (bezpłatnie)
Eurobank	token (0–2 zł/mies.), token GSM (0–0,5 zł/mies.)
Idea Bank	hasła SMS (bezpłatnie)
ING	hasła SMS (bezpłatnie)
Getin Bank	hasła SMS (bezpłatnie)
Kredyt Bank	lista kodów (8 zł), token (50 zł), token GSM (bezpłatnie)
mBank	lista kodów (9 zł), hasła SMS (bezpłatnie)
Meritum Bank	hasła SMS (bezpłatnie), token (60 zł)
Millennium	hasła SMS (bezpłatnie)
MultiBank	hasła SMS (bezpłatnie)
Nordea Bank	lista kodów (bezpłatnie), token (20 zł/mies. przez pierwszy rok, potem bezpłatnie), kwalifikowany podpis elektroniczny (366,54 zł za pierwsze dwa lata)
Pekao SA	hasła SMS (0–0,2 zł za hasło), token (1 zł/mies.), token GSM (bezpłatnie), dodatkowo dla starych klientów lista kodów (bezpłatnie)
PKO BP (także Inteligo)	lista kodów (bezpłatnie), hasła SMS (bezpłatnie), token GSM (bezpłatnie)
Toyota Bank	token (bezpłatnie)
Volkswagen Bank direct	token (bezpłatnie lub 36 zł rocznie, w zależności od typu rachunku)

Źródło: Cerega (2012).

Spośród 24 banków, które znalazły się w zestawieniu Idea Expert, aż 18 stosuje do autoryzacji przelewów internetowych hasła SMS. W sześciu z nich (BZ WBK, Getin Banku, Idea Banku, ING, mBanku i Millennium) jest to jedyna dostępna metoda. 11 kolejnych daje klientom także inne zabezpieczenia do wyboru (w tym tak niestandardowe, jak możliwość odsłuchania hasła jednorazowego w systemie IVR, proponowana przez Citi Handlowy). Ciekawy jest przypadek BPH, w którym korzystanie z haseł SMS jest niezbędne, ale samo w sobie nie wystarcza, by wykonać przelew zewnętrzny. Bank zdecydował, że bezpieczeństwo jest ważniejsze niż wygoda użytkownika i stosuje dwustopniowe zabezpieczenie. Ta sama transakcja jest potwierdzana zarówno podpisem elektronicznym, jak i kodem SMS. Dziewięć instytucji pozostawiło możliwość posługiwania się hasłami z tradycyjnej listy, osiem proponuje korzystanie z tokena sprzętowego. Mniej popularne są na razie tokeny GSM, jednak można się spodziewać, że kolejne banki będą sięgały po to rozwiązanie (Cerega, 2012). Szczegółowe zestawienie metod autoryzacji przelewów internetowych zawarto w tabeli 1.

Podsumowanie

Podsumowując należy stwierdzić, że bankowość i informatyka stały się dziedzinami nierozerwalnie ze sobą związanymi, a ich ścisła integracja charakteryzuje się znaczną dynamiką. Z jednej strony ekspansja technologii informatycznych otwiera przed bankami nowe możliwości, z drugiej zaś rosnące potrzeby banków i innych instytucji finansowych, związane przede wszystkim z bezpieczeństwem przetwarzania i przesyłania danych w postaci elektronicznej, stymulują rozwój i doskonalenie tych technologii. Ponadto ów złożony charakter bezpieczeństwa obejmuje również swym zasięgiem problemy techniczne, technologiczne, organizacyjne, prawne oraz ekonomiczne (Węsierska E., 2004, s. 135).

W raporcie Bankier.pl (Macierzyński, 2009) **„Bezpieczeństwo bankowości internetowej w Polsce”** zamieszczono dokładny przegląd stosowanych przez banki zabezpieczeń. Wynika z nich, iż obecnym trendem we wszystkich bankach w Polsce jest dwustopniowy poziom zabezpieczeń – jeden do logowania do rachunku, drugi do potwierdzania transakcji. Do najpopularniejszych sposobów autoryzacji należy zaliczyć hasła jednorazowe, hasła SMS-owe, czy tokeny. Wszystkie te sposoby oferują bardzo silne zabezpieczenie. Najsłabszym ogniwem w systemie jest końcowy użytkownik. Większość zabezpieczeń staje się bezwartościowa, jeśli klient dobrowolnie przekaże hasła złodziejowi lub niedostatecznie

zadba o zabezpieczenie swojego komputera. Banki próbują tej prostej zasadzie przeciwdziałać, ale każde zwiększenie bezpieczeństwa odbywa się kosztem wygody użytkowania, a przede wszystkim kolejnymi wydatkami, które ostatecznie przerzucane są na klienta. Dlatego instytucje finansowe próbują wypośrodkować te dwa elementy – wygodę i bezpieczeństwo, chociaż mają świadomość, że przy obecnej masie klientów zwykłe prawdopodobieństwo sprawia, że może dojść do kradzieży haseł.

Z raportu Bankier.pl (Macierzyński, 2009) wynika, że porównując nasze banki do tych zagranicznych, można śmiało orzec, że stosują najwyższe standardy bezpieczeństwa, ale także cały czas pracują nad ulepszeniem już istniejących zabezpieczeń. W kwestiach bezpieczeństwa, cały czas trwa nieustanny wyścig.

Bibliografia

Bilski T. (2000), *Nowe narzędzia do ochrony systemów informatycznych w bankowości*, w: red. A. Gospodarowicz, *Zastosowania rozwiązań informatycznych w bankowości*, Wydawnictwo Akademii Ekonomicznej we Wrocławiu, Wrocław.

Bogacka-Kisiel E. red. (2000), *Usługi i procedury bankowe*, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław.

Cerega P. (2012), Idea Expert, BankierPress www.bankier.pl/wiadomosc/Telefon-bywa-niezbedny-zeby-wykonac-przelew-2656859.html (dostęp 15.02.2014).

Chmielarz W. (2005), *Systemy elektronicznej bankowości*, Difin, Warszawa.

Grobicki J. (2005), *Wirtualne, czyli realne straty*, „Bank", nr 7–8, s. 63–64.

Grzywacz J. (2004), *Bankowość elektroniczna w działalności przedsiębiorstwa*, Szkoła Główna Handlowa w Warszawie, Warszawa.

Hanusik A., Machulik R. (2004), *Norma bezpieczeństwa e-banking, oczekiwania i wymagania z punktu widzenia potrzeb klienta*, w: red. A. Gospodarowicz, *Zastosowania rozwiązań informatycznych w instytucjach finansowych*, Prace Naukowe nr 1035, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław.

Hołownia P. (2007), *Zrozumieć także klienta*, „Bank", nr 1, s. 22–25.

Jurkowski A. (2001), *Bankowość elektroniczna*, Narodowy Bank Polski, Materiały i Studia, Zeszyt nr 125, Warszawa.

Koźliński T. (2004), *Bankowość internetowa*, CeDeWu Sp. z o.o., Warszawa.

Macierzyński M, (2009), *Najnowocześniejsze zabezpieczenia w bankowości internetowej*, Bankier.pl, www.bankier.pl/wiadomosc/Raport-Bankier-pl-Najbezpieczniejsze-banki-internetowe-2034334.html (dostęp 15.02.2014).

Michalski A. (2002), *Wykorzystanie technologii systemów informatycznych w procesach decyzyjnych,* Politechnika Śląska, Gliwice.

Samcik M. (2006), *Testujemy bezpieczeństwo internetowych kont bankowych*, „Gazeta Wyborcza", 20.11.2006, http://gospodarka.gazeta.pl/gospodarka/2029020,33181,3744366.html (dostęp 15.02.2014).

Wawrzyniak D. (2005), *Bezpieczeństwo bankowości elektronicznej*, red. A. Gospodarowicz, *Bankowość elektroniczna*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Węsierska E. (2004), *Dywersyfikacja metod ochrony systemów elektronicznych jako warunek funkcjonowania przedsiębiorstwa bankowego*, w: red. A. Gospodarowicz *Zastosowania rozwiązań informatycznych w instytucjach finansowych*, Prace Naukowe nr 1035, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wrocław.

Włodarczyk E. (2007), *Certyfikat nie do złamania*, „Bank", nr 5, s. 48–49.

Wroński P. (2004), *Bankowość elektroniczna dla firm*, CeDeWu, Warszawa.

SECURE ONLINE BANKING SERVICES

Summary

Banks are aware of the fact that the traditional form of communication with the customer does not meet the needs of all declared and often downright uncomfortable. A natural consequence of this is so getting stronger relationship banking IT environment, allowing for effective overcome the barriers of time and space, which, however, one of the basic rules is an adequate level of data protection. At present, therefore, it was necessary to develop new ways of securing business transactions, largely made electronically, from potential abuse. No guarantee an adequate level of security of their newly created varieties do not have any chance to spread, whether or not the implementation. At the same time, due to the fact that the security methods continue to evolve or are replaced with newer, it's hard to say that they are tested.

Translated by Marcin Bitdorf

Keywords: safety, risk, web services