Problemy bezpieczeństwa w bankowości internetowej

Katarzyna Anna Lewkowicz*

Gwałtowne zwiększenie liczby transakcji oraz wzrost wymagań klientów spowodowały, że banki stały się prekursorami w stosowaniu najnowszych technik komputerowych. Konieczność sprostania konkurencji powoduje potrzebę rozwijania zarówno poziomu usług, technologii, jak i jakości informacji. Wszystko to, w połączeniu ze stosowaniem coraz bardziej złożonych i rozległych systemów informatycznych, rodzi nowe problemy związane z bezpieczeństwem informacji. W szczególności z zapewnieniem poufności i integralnych danych, potwierdzeniem autentyczności i niezaprzeczalności nadawcy czy odbiorcy. Szeroki rozwój tzw. bankowości elektronicznej stwarza jednak wiele niebezpieczeństw związanych z użyciem systemu informatycznego przez osoby nieuprawnione. Stale zresztą zwiększa się w Polsce liczba prób penetracji systemów informatycznych zarówno przez entuzjastów informatyki, jak i wyspecjalizowanych przestępców komputerowych, wykorzystujących systemy informatyczne do nieuczciwych celów [2, s. 48]. Celem niniejszego artykułu jest analiza bezpieczeństwa informatycznego w polskich bankach ze szczególnym uwzględnieniem bankowości internetowej.

W okresie ostatnich kilku lat nastąpił dynamiczny rozwój bankowości elektronicznej. Nowoczesna technika a przede wszystkim szybki rozwój informatyki umożliwiły dokonywanie większości transakcji bez konieczności przemieszczania się i dostarczania dokumentów w formie papierowej. Dla kierunku rozwoju bankowości elektronicznej ważne jest przede wszystkim zastosowanie coraz nowszych i szybszych form komunikowania. Nie chodzi w tym przypadku jedynie o parametry techniczne, ale też o zapewnienie bezpieczeństwa oraz usuwanie istniejących barier prawnych.

Najważniejszym zadaniem warunkującym rozwój i efektywność bankowej informatyki było zorganizowanie wyspecjalizowanej sieci teletransmisji łączącej jednolitym systemem wszystkie banki. Taką rolę w Polsce odgrywa od kilku lat system ELIXIR. Drugim, również ważnym elementem rozwoju była i jest kompleksowa informatyzacja central i poszczególnych oddziałów operacyjnych banków, co umożliwia ich włączenie do systemu teletransmisji. Komunikacja pomiędzy bankiem a przedsiębiorstwem odbywa się najczęściej za pomocą linii

* Mgr Katarzyna Anna Lewkowicz, doktorantka w Uniwersytecie w Białymstoku.

telekomunikacyjnych, a przesyłane dane są odpowiednio kodowane. Niektóre programy w zakresie obsługi i komunikacji funkcjonują przy wykorzystaniu łącz i funkcjonalności Internetu. Z punktu widzenia dostępu do informacji systemy można podzielić na działające w trybie [4, s. 62]:

- On-line – przepływ informacji i aktualizacja baz odbywa się w sposób ciągły;
- Off-line – informacje są przygotowywane, przesyłane oraz pobierane okresowo, w związku z czym aktualizacja informacji, w zależności od określenia ich zakresu następuje po każdorazowej transmisji. W praktyce komunikacja odbywa się 1–3 razy dziennie (czasami częściej – zależnie od doraźnych potrzeb przedsiębiorstwa).

Z punktu widzenia przedsiębiorstwa najbardziej istotną cechą każdego systemu jest bezpieczeństwo transakcji oraz przesyłanych i przechowywanych informacji. Stosowane rozwiązania muszą być stale modyfikowane oraz zawierać wiele etapów weryfikacji i kontroli praw dostępu. Szczególne znaczenie mają sposoby zabezpieczeń przy wykorzystaniu połączeń internetowych, do których dostęp jest powszechny i praktycznie nieograniczony. We wszystkich przypadkach istotna jest nie tylko ocena zastosowanych zabezpieczeń, ale także zagwarantowana w umowie odpowiedzialność lub współodpowiedzialność banku w przypadku powstania szkód w wyniku złamania zabezpieczeń albo wystąpienia awarii technicznych.

Kwestia bezpieczeństwa miała i ma kluczowe znaczenie w bankowości. W przypadku bankowości tradycyjnej istnieją takie sposoby jak odręczny podpis, czy wylegitymowanie przy pomocy dowodu osobistego bądź innego dowodu tożsamości. Są one powszechnie przyjęte, akceptowane i uważane za sprawdzone przez co nawet nikt nie próbuje ich kwestionować. Jednak te sposoby nie są możliwe do bezpośredniego przełożenia na realia bankowości elektronicznej ze względu na odmienne możliwości człowieka i maszyny (automatu). Na przykład weryfikacja odręcznego podpisu, który powinien być zgodny ze wzorem, ale nigdy nie będzie z nim identyczny, jest dla człowieka kwestią spojrzenia i osądzenia. Natomiast dla maszyny jest to kwestia skanowania podpisu (co jest zawsze ograniczone rozdzielczością skanera) i porównania za wzorem. W tej sytuacji konieczne stało się wypracowanie innych nowych sposobów na zabezpieczenie transakcji bankowych dokonywanych drogą elektroniczną przed możliwymi nadużyciami.

Wszystkie rodzaje stosowanych zabezpieczeń można przyporządkować następującym metodom służącym zapewnianiu bezpieczeństwa [3]:

- szyfrowana transmisja danych;
- proste uwierzytelnianie, czyli uwierzytelnianie oparte na czymś, co się posiada (np. wszelkiego rodzaju hasła);
- silne uwierzytelnianie, czyli uwierzytelnianie oparte na czymś, co się posiada (np. certyfikat, token, klucz prywatny);
- podpis elektroniczny.

Pierwsza metoda jest ściśle związana z kryptografią, a jej stosowanie ma na celu uniemożliwienie dostępu osobom nieupoważnionych do poufnych danych przesyłanych drogą elektroniczną. Druga i trzecia metoda służą identyfikacji stron transakcji i ma na celu uniemożliwienie zaistnienia sytuacji, w których jedna osoba „podszywa się" pod inną osobę. Z kolei czwarta metoda ma związek z zasadą niezaprzeczalności. Podpis elektroniczny pełni funkcję uwierzytelniania strony transakcji.

Bezproblemowe korzystanie z nowych rodzajów bankowości elektronicznej z czasem wywołuje u klientów wzrost zaufania, co bezpośrednio wpływa na ich poczucie bezpieczeństwa do nowych form usług bankowych. Bezpieczeństwo w dokonywaniu operacji to nie tylko uniemożliwienie dostępu do konta osobie nie będącej jego właścicielem lub pełnomocnikiem. Chodzi również o zachowanie tajemnicy bankowej, a także o prawidłowość danych przesyłanych droga elektroniczna. Rolą stosowanego systemu zabezpieczeń jest wypełnianie następujących zadań [3]:

- uniemożliwienie dokonywania transakcji na rachunkach przez osoby niepowołane;
- uniemożliwienie osobom nieuprawnionym „podglądania" transakcji, kont oraz dostępu do innych danych podlegających prawnej ochronie lub tajemnicy bankowej;
- chronienie składanych zleceń przed zniekształceniem w trakcie transmisji;
- uniemożliwienie wyparcia się przez klienta dokonanych transmisji (tzw. niezaprzeczalność).

W systemach bezpieczeństwa dużą role odgrywa czynnik czasu. Systemy te bazują na technice, która charakteryzuje się stosunkowo szybkim postępem. Stosowane dzisiaj rozwiązania mogą być wystarczające, ale nie będą w przyszłości. Ciągły postęp techniczny pozwala na stosowanie coraz bardziej zaawansowanych zabezpieczeń przez banki. Jednocześnie daje coraz to większe możliwości osobom o nieczystych zamiarach. Ważne dla banku jest stałe nadążanie za postępem technologicznym i dostosowywanie systemu bezpieczeństwa do zmieniającej się rzeczywistości.

Transakcje w bankowości internetowej realizowane są za pośrednictwem otwartej i ogólnodostępnej sieci jaką jest Internet. Zmniejsza to koszty i ułatwia dostęp. Jednak jest także źródłem pewnych zagrożeń. Z otwartej natury Internetu wynika, że strony wymiany informacji nie maja kontroli nad drogą ich przesyłu. Istnieje techniczna możliwość przechwycenia komunikacji między komputerami klienta i banku. Ponadto system komputerowy banku podłączony do Internetu wystawia go na ataki włamywaczy. Mogą oni próbować podejrzeć dane. Liczne i nagłaśniane przez środowisko masowego przekazu przypadki włamań do komputerowych powodują, że wiele osób podchodzi do przekazywania poufnych danych przez Internet z dużą rezerwą. Aby zdobyć zaufanie deponentów, bank internetowy musi nie tylko zastosować odpowiednie technologie kryptograficzne

i odpowiednio zabezpieczyć swoje komputery przed niepowołanym dostępem, ale i przekonać o skuteczności swoich działań klientów.

Komunikacja między komputerem klienta i banku musi być zatem prowadzona z zastosowaniem technik kryptograficznych zapewniających spełnienia trzech podstawowych warunków bezpieczeństwa [4]:

- szyfrowanie danych w taki sposób, by osoby trzecie nie mogły ich odczytać, nawet jeśli uda im się je przechwycić;
- możliwość sprawdzenia, czy podczas przesyłania dane nie zostały zmienione;
- zapewnienie wiarygodnej autoryzacji danych przez nadawcę, tak by mogły być traktowane przez odbiorcę jako prawnie wiążące dyspozycje- tak zwane podpisy elektroniczne.

Szyfrowanie komunikacji między bankiem a klientem powinno być oparte głównie na standardowych, ogólnie dostępnych i rozpowszechnianych rozwiązaniach. Takim standardowym rozwiązaniem, stosowanym powszechnie przez banki i inne instytucje finansowe, jest wprowadzony przez firmę Netscape system Secure Sockets Layer (SSL)[1]. Stosunkowo niewiele banków polega wyłącznie na protokole SSL. Istnieje wiele rozwiązań używanych do wzmocnienia owego protokołu. Ogólnie można podzielić je na trzy grupy [4]:

- rozwiązania sprzętowe;
- rozwiązania programowe bazujące na tzw. plu-ins;
- rozwiązania programowe używające technologii Java.

Rozwiązanie sprzętowe to przede wszystkim karty chipowe i technologie MeCHIP. Są one używane głównie w celu ochrony i przechowywania klucza szyfrującego. Proste karty pamięciowe, analogiczne do kart telefonicznych, służą jedynie do zapisania klucza. Wszystkie obliczenia związane z jego weryfikacją przeprowadzane są przez komputer. Z kolei w przypadku kart „inteligentnych" (smart cards) – zawierają one proste, ale samodzielny komputer, który sam wykonuje wszystkie obliczenia.

Nazwą plug-in (ang. „wtyczka") określany jest niesamodzielny program rozszerzający funkcjonalność przeglądarki i z nią zintegrowany. Przeznaczony jest zawsze do działania w konkretnym systemie operacyjnym, choć bank może przygotować wersje dla różnych systemów. Plug-in może być instalowany na komputerze klienta z dyskietki czy CD-ROMu, lub za pośrednictwem Internetu. W tym ostatnim przypadku ważne jest zapewnienie wiarygodności źródła, z którego klient pobiera program aby wykluczyć podszywanie się innego komputera pod serwer banku.

Rozwiązania używające języka Java polegają na rozszerzeniu funkcjonalności przeglądarki i różnią się jednak znacząco od wtyczek. Po pierwsze, odpowiedni program (zwany niekiedy w tym kontekście appletem) jest zawsze ładowany z Internetu. Ułatwia to aktualizację i nie wiąże klienta z konkretnym komputerem, nie wymagają też żadnych dodatkowych komponentów sprzętowych.

[1] SSL jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych.

W razie odkrycia luki w systemie bezpieczeństwa można je automatycznie aktualizować, nie niepokojąc tym klientów.

Banki starają się zainstalować takie rozwiązania, które zapewnią maksimum bezpieczeństwa wszystkich danych i transakcji. Jednak nigdy nie można mieć pewności, że bank stosuje rozwiązania najlepsze, bo będzie zasłaniał się tu tajemnicą. Ale nawet jeżeli zabezpieczenia będą na najwyższym poziomie i tak stuprocentowej gwarancji nie będzie. Poniżej opisano wybrane zasady działania systemów zabezpieczeń w bankowości internetowej. Transmisja danych między komputerem klienta banku a jego serwerem jest szyfrowana za pomocą specjalnego protokołu SSL. Dla każdego połączenia tworzone są klucze wykorzystywane tylko raz. Bankowy serwer ma specjalny certyfikat, który gwarantuje, że klient łączy się z bankiem a nie z komputerem. O bezpieczeństwie połączenia decyduje między innymi wspomniany wyżej jednorazowy klucz. Im jest on dłuższy, tym lepiej dla bezpieczeństwa transmisji [6].

Z kolei numer klienta i hasło dają pewność, że z systemu korzysta uprawniona osoba. Istnieje jednak niebezpieczeństwo podejrzenia hasła przez osoby obce. Dlatego banki często stosują dodatkowe hasło jednorazowe. Generuje je specjalne urządzenie o nazwie token. Po wpisaniu przez klienta do niego ciągu cyfr dostępnego na stronie internetowej banku podczas logowania do systemu. Wygenerowane przez token hasło należy następnie wpisać do przeglądarki internetowej. Dopiero wpisanie prawidłowego hasła z tokena umożliwia wejście do systemu. Zaletami tokena są unikalne hasła, i żaden wirus komputerowy nie ma szans kradzieży tych haseł ponieważ tokena w żaden sposób nie podłączamy do komputera. Jeżeli nawet komuś uda się poznać hasło ma to znaczenie tylko przez parę chwil, gdyż hasło to jest ważne przez krótki moment. Następnie bankowy system unieważnia je [7].

Istotą nowoczesnych technologii bankowości jest połączenie kryptografii symetrycznej i niesymetrycznej, tak aby wykorzystać zalety i równocześnie wyeliminować wady każdej z nich. W metodzie niesymetrycznej każda ze stron wirtualnej transakcji ma dwa wzajemnie się uzupełniające i tworzące parę klucze – tzw. klucz prywatny i klucz publiczny. Jakakolwiek wiadomość zaszyfrowana przy użyciu jednego może zostać odczytana wyłącznie przy użyciu drugiego. I na odwrót.

Jednocześnie klucz stosowany do zakodowania wiadomości nie pozwala na jej odszyfrowanie. Każdy ma więc klucz prywatny, znany tylko sobie i tzw. publiczny, całkowicie jawny. Chcąc wysłać komuś wiadomość, koduje się ją, korzystając z ogólnie dostępnego klucza publicznego tej osoby. Odczytać informację będzie mógł jednak wyłącznie jej adresat, bo tylko on posiada klucz prywatny. Kryptografia niesymetryczna umożliwia generowanie elektronicznych podpisów, co pozwala stwierdzić czy nikt nie podszywa się pod nadawcę. W praktyce oznacza to, że jeżeli wiadomość zakoduje się przy użyciu klucza prywatnego, adresat – dysponując kluczem publicznym nadawcy – może ją rozszyfrować. Ma przy tym pewność, że przekaz pochodzi od tej właśnie osoby, bowiem tylko ona dysponuje kluczem prywatnym. Co więcej: nadawca nie może

zaprzeczyć, że to właśnie on wysłał wiadomość. W kryptografii symetrycznej istotną zaletą jest natomiast szybkość, wydajność oraz odporność na wszelki włamania osób nieuprawnionych [5].

System komputerowy banku musi być zabezpieczony przed próbami penetracji z zewnątrz. Jakość i pewność tego zabezpieczenia jest dla banku internetowego czynnikiem o decydującym znaczeniu. Nawet jedna ujawniona próba włamania uwieńczona sukcesem mogłaby bowiem całkowicie podkopać zaufanie klientów. Zapewnienie bezpieczeństwa jest tu o tyle trudne, że ze zrozumiałych przyczyn część systemu informatycznego musi być dostępna z zewnątrz dla klientów załatwiających swoje interesy. Bank musi więc zrealizować dwa przeciwstawne cele: z jednej strony umożliwić klientom jak najszerszy dostęp do dotyczących ich danych, z drugiej-odciąć wszelką nieuprawnioną komunikację z Internetu do swojego wewnętrznego systemu komputerowego. Realizowane jest to przy pomocy technologii firewall („ściana ogniwa"). Polega ona na stałym filtrowaniu danych przechodzących z zewnątrz do wewnętrznej sieci banku i nieprzepuszczaniu jakichkolwiek informacji pochodzących z nieznanych czy nieuprawnionych źródeł. Komunikacja z zewnątrz adresowana jest do systemu firewall, który po sprawdzeniu przekazuje ją dalej. Wewnętrzna struktura sieci komputerowej banku pozostaje niewidoczna z zewnątrz

Rzeczywisty poziom bezpieczeństwa w usługach bankowości elektronicznej nie jest tożsamy z poczuciem bezpieczeństwa u klientów banku. Jest on zależny od zastosowanych rozwiązań oraz ich szczegółów technicznych. Natomiast poczucie bezpieczeństwa dokonywanych drogą elektroniczną transakcji bankowych u klientów wiąże się bardziej z ich subiektywnymi odczuciami. Te z kolei najbardziej uzależnione są od zasłyszanych opinii oraz przypadków nadużyć. Przyczyną tych rozbieżności jest najczęściej niewiedza samych klientów oraz ich strach przed rzeczami nowymi. Wiedza potrzebna do oceny systemu bezpieczeństwa stosowanego przez bank wykracza poza zakres wiedzy przeciętnego klienta. Liczne i nagłaśniane przypadki włamań hakerskich do systemów komputerowych należących nawet do dużych i znanych korporacji (chociaż zazwyczaj nie chodzi o banki) również znajdują odbicie w świadomości klientów banku. Stosowany system zabezpieczeń wzbudzi zaufanie klientów, jeśli sprawdzi się w praktyce. Taki proces potrzebuje jednak czasu.

Literatura

1. Grzechnik J., *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk 2000.
2. Grzywacz J. *Bezpieczeństwo systemów a ryzyko banku*, „Bank" 1999, nr 12.
3. Jurkowski A., *Bankowość elektroniczna*, Materiały i studia, Warszawa czerwiec 2001, zeszyt nr 125.
4. Tomala P., *Systemy home banking*, „Bank" 2002, nr 7–8.
5. www.businessman.onet.pl/artykuł.html?ITEM=100933
6. www.ebanki.pl/technika/ssl.html/
7. www.ebanki.pl/technika/uwierzytelnianie.html/