Daniel Wiśniewski

Państwowa Wyższa Szkoła Zawodowa we Włocławku

Ryzyka klienta bankowości elektronicznej

The risk of customer electronic banking

Streszczenie

Bankowość elektroniczna jest częścią współczesnej bankowości. Ciągły jej rozwój ułatwia korzystanie z usług bankowych. Daje to również nowe możliwości kradzieży środków z kont bankowych. W tych warunkach za szczególnie istotne uznać trzeba zabezpieczenie ważnych informacji zawartych na serwerach banków. Należy więc chronić każdą operację wykonywaną na koncie bankowym przed atakami złodziei w świecie realnym, jak i w świecie wirtualnym.

Słowa kluczowe: bankowość elektroniczna, bank, zabezpieczenia, zagrożenia, konto bankowe

Abstract

Electronic banking is a part of modern bank system. Its continuous development facilitates the use of banking services. This also gives the new possibilities for stealing funds from the bank accounts. It is also important to take care of the security of main information contained on the servers of banks. It is therefore necessary to protect any operations performed on the bank account against attacks by thieves in the real world and the virtual world.

Keywords: electronic banking , bank, security, threats, bank account

1.1. Wstęp

Celem poniższego opracowania jest udowodnienie następującej hipotezy badawczej:

Nieustanny rozwój bankowości powoduje zwiększenie ryzyka utraty środków na koncie bankowym.

Każda nowa technologia umożliwiająca innowacyjny sposób komunikacji z bankiem, tworzy również szanse na przełamanie zabezpieczeń i skuteczne włamania do systemu bankowego. Zostaną przedstawione zarówno rodzaje zabezpieczeń stosowanych przez banki, jak i sposoby ich przełamywania, co skutkuje kradzieżą pieniędzy ulokowanych na kontach bankowych.

1.2. Zabezpieczenia systemów bankowości elektronicznej

Punktem wyjścia wywodów uczyniono omówienie sposobów zabezpieczania systemów bankowych. Podstawowym systemem wykorzystywanym przez banki są specjalne protokoły i szyfrowanie danych. Jednym z najczęściej stosowanych jest *Secure Socket Layer*[1]. Jego twórcą jest *Netscape Communication*. Funkcjonuje on powyżej warstwy transportowej Internetu i jednocześnie poniżej warstwy aplikacji. Jest najłatwiejszym sposobem zabezpieczeń komunikacji pomiędzy bankiem, a klientem. W tym przypadku, osoba, która legalnie chce się połączyć z serwerem banku dostaje klucz publiczny, służący do szyfrowania trwającej w tym czasie sesji. Gdy użytkownik chce ponownie się połączyć, dostaje nowy klucz szyfrujący. Dla bezpieczeństwa transakcji, protokół sprawdza nie tylko serwer, ale także użytkownika. Ma to na celu zapobieganie podszywaniu się pod klienta banku. W tym celu stosuje się certyfikaty. Cały proces składa się z kilku etapów. Na początku serwer banku wysyła swój certyfikat, zaś komputer klienta sprawdza go. Następnie zostaje wygenerowany klucz, pozwalający na określenie metody kryptograficznej jak i jego długość. Następnie z uzyskanych informacji tworzony jest klucz

[1] A. Matuszyk, P.G. Matuszyk, *Instrumenty bankowości elektronicznej*, Warszawa, 2011, s. 99.

sesyjny i wysyłany do serwera banku[2]. Przestawiona metoda nie jest doskonała, w efekcie dochodzi do złamania tego protokołu. Nie można ustalić skali tego procederu, ze względu na nie ujawnianie tych informacji przez banki. Właśnie dlatego stosuje się dwa poziomy zabezpieczeń. Jako pierwsze brane jest pod uwagę oprogramowanie jak i sprzęt, zaś drugie opiera się na kontroli pracowników banku oraz samej procedurze bezpieczeństwa. Jako pierwsza zostanie omówiona część bezpieczeństwa związana ze sprzętem. Na początku określa się jakie niebezpieczeństwa związane są ze sprzętem i oprogramowaniem oraz jakie środki są potrzebne do jego zabezpieczenia. Następnie ustala się zakres możliwości ingerencji lub dostępu poszczególnych osób do plików w części oprogramowania. Kolejnym etapem jest generowanie raportów z pomocą przeznaczonego dla tego celu programu. Dla zwiększenia bezpieczeństwa wszelkie informacje są szyfrowane w celu uniknięcia ujawnienia poufnych danych. Ostatnim i nie miej ważnym elementem jest zdublowanie systemu, pozwalającego na nieprzerwaną pracę. W tym celu stosuje się inny komputer lub serwer. Drugi poziom obejmuje użytkowników jak i zasady bezpieczeństwa. Również składa się z kilku elementów. Jednym z pierwszych jest identyfikacja użytkownika, związana z dostępem do danych. Sprawdzany jest jego zakres ingerencji w system. W tym celu stosuje się odciski palca, kody PIN, rozpoznawanie głosu oraz inne tego typu metody. Kolejnym elementem jest autoryzacja osoby, realizacja zlecenia oraz rozliczenie tej operacji pomiędzy bankami[3]. Ważnymi cechami potrzebnymi do bezpiecznego prowadzenia systemu to poufność, integralność, autentyczność, niezaprzeczalność, dostępność i niezawodność. Tylko zrozumienie i wprowadzenie tych cech pozwoli na bezpieczne korzystanie z bankowości elektronicznej. Trudnością związaną z kolejnością ich wdrażania jest system wartości poszczególnych osób. Dla jednego klienta część z tych cech może być ważniejsze od reszty, zaś dla innego ważne są inne kryteria. Dlatego w tym celu wprowadzono standaryzację. Międzynarodowa Organizacja Standaryzacyjna jest jedną z najważniejszych. Tworzy ona normy dla różnych dziedzin. Za przykład niech posłużą standardy ISO 7341:1985, ISO

[2] A. Gospodarowicz, *Bankowość elektroniczna,* Warszawa 2005, s. 95-96.
[3] A. Matuszyk , P.G. Matuszyk, *Instrumenty..,* s. 99-101.

8730:1990 oraz ISO 13491-1:1998. Do ważniejszych można zaliczyć *American National Standard Institute*(ANSI), *National Institute of Standards and Technology*(NIST) czy I*nstitute of Electrical and Elektronic Engineers*(IEEE). Również w Polsce znajduje się instytucja zajmująca się tworzeniem standardów. Jest nim Polski Komitet Normalizacyjny. Powyższe standardy nie posiadają mocy prawnej. Pozwalają jednak wskazać kierunek działań w jaki sposób przygotować i wdrożyć system w części organizacyjnej oraz technicznej[4]. W celu zabezpieczania danych zawartych na serwerach stosuje się wiele środków ochrony. Pierwszymi z nich są fizyczne środki ochrony. Są to wszelkie urządzenia lub przedmioty uniemożliwiające dostęp do danych. Są nimi sejfy, alarmy, systemy przeciwwłamaniowe, systemy przeciwpożarowe i tymu podobne. Kolejnym środkiem jest zabezpieczenie techniczne. Zalicza się do nich wszelakie karty magnetyczne i mikroprocesorowe, urządzenia sprawdzające linie papilarne, maszyny do podtrzymywania zasilania, czy wytwarzania kopii zapasowych, serwery Proxy i tak dalej. Następnym jest programowe zabezpieczenie systemu. Do tej grupy zaliczamy dzienniki systemowe, oprogramowanie określające kto wykonuje operacje,*firewall,* wirtualne sieci prywatne, programy antywirusowe. Kolejnym jest organizacyjny środek ochrony, w skład którego wchodzą szkolenia pracowników, wykorzystana przez bank polityka bezpieczeństwa, badanie ryzyka, kontrola systemu oraz wykrywanie odchyleń. Kolejnym jest kontrola dostępu. Polega ona na sprawdzeniu i kontrolowaniu osób wykorzystujących system bankowy. Użytkownik może wiedzieć o systemach zabezpieczeń lub posiadać element tego systemu. Częścią tego jest również identyfikacja osoby, próbującej zalogować się do systemu. Na początku omówione zostaną elementy, o których wie lub je posiada klient banku. Opisywane systemy można podzielić ze względu na powszechności ich stosowania. Pierwszym z nich są hasła, którymi klient posługuje się, aby połączyć się z serwerem banku. Kolejnym jest zastosowanie częściowych kodów podanych przez bank za pomocą specjalnego generatora. Następne są kody jednorazowe zawarte na specjalnej liście, które mogą być niejawne lub jawne. Wykorzystuje się również kryptograficzne karty elektroniczne. Bardzo interesującym

[4] A. Gospodarowicz, *Bankowość...*, s. 55-59.

rozwiązaniem kontroli dostępu użytkownika jest używanie tokenu jako elementu potrzebnego do autoryzacji[5]. Jest on specjalnym urządzeniem, dzięki któremu możliwa jest identyfikacja użytkownika. Często ów sprzęt przypomina wyglądem brelok do kluczy lub mały kalkulator. Jego zadaniem jest generowania ciągu cyfr potrzebnych, aby posiadacz tokena mógł wykonywać operacje na swoim koncie bankowym. Urządzenie to powiązane jest tylko z jednym kontem bankowym i tylko z nim można go używać. Funkcjonuje ono na zasadzie kluczy i algorytmów kryptograficznych. Otrzymany kod z urządzenia opierany jest na prywatnym kluczu, czasie oraz bazie zapisanych w nim kodów. System bankowy wiedząc o kluczach prywatnych i wykorzystanych przez token algorytmach, potrafi zidentyfikować użytkownika. Owe urządzenia tworzy wiele firm, jednakże nie zdradzają ich budowy, ze względu na ryzyko złamania zabezpieczeń i co umożliwiałoby kradzieże[6]. Kolejnym zabezpieczeniem jest podpis elektroniczny. Jest on swoistym podpisem cyfrowym, który pełni tę samą funkcję co podpis tradycyjny. Wykorzystuje on jednokierunkowe funkcje matematyczne, składające się z ciągu bitów, który jest dołączany do przesłanych danych. Kolejność tworzenia tego podpisu oraz jego weryfikacja przebiega w następujący sposób. Po pierwsze, plik danych jest przetwarzany na ciąg bitów. Następnie te dane przy pomocy funkcji matematycznej tworzoną unikalną wartość *hash.* Otrzymany ekstrakt jest zakodowany przez klucz nadawcy i otrzymany kryptogram przedstawia podpis elektroniczny. Paczka danych jest wysyłana do odbiorcy, następnie ta wiadomość generuje wartość *hash*. Ten plik zostaje odszyfrowany przy pomocy klucza publicznego nadawcy. Jeśli wynik tej operacji jest prawidłowy, to sprawdzenie kończy się wynikiem twierdzącym. Popularniejszą metodą zabezpieczeń staje się weryfikacja za pomocą części ciała użytkownika takie jak układ linii papilarnych, geometria dłoni, brzmienie głosu czy obraz tęczówki oka. W przypadku odcisku palca polega to na skanowaniu odpowiedniego obszaru specjalnym skanerem, który sprawdza punkty charakterystyczne z zapisanym wzorcem. Metoda ta może również być poszerzona o technologie badania pojemności elektrycznej skóry w danym punkcie,

[5] Tamże s.77-80.
[6] http://home.agh.edu.pl/~woznicki/tokeny.html (dostęp 02.04.2016).

który jest trudniejszy do oszukania. W przypadku geometrii dłoni sposobem weryfikacji jest konfrontacja z trójwymiarowym jej zdjęciem. W tym przypadku sprawdza się długość, szerokość, grubość czterech palców oraz wielkość obszarów pomiędzy kostkami. Wykorzystuje on ponad 90 różnych cech charakterystycznych.

Jednym z najbardziej niepowtarzalnym identyfikatorów jest tęczówka oka. Kształt jej zostaje nadany w ciągu drugiego roku życia i pozostaje taki sam do końca życia. Tęczówka posiada 266 punktów charakterystycznych, dając ogromną liczbę kombinacji. Owe systemy biometryczne można obecnie traktować jako nowinkę technologiczną, gdyż koszt wprowadzenia tej technologii nie pozwala na jej spopularyzowanie. Rozwój tych systemów bezpieczeństwa pozwala na systematyczne obniżenie kosztów i w efekcie spopularyzowanie tych technologii[7].

1.3. Klasyfikacja zagrożeń

W tej części zostaną omówione sposoby atakowania systemów bankowych oraz dokonywania kradzieży danych z kart bankowych, a także wyłudzania pieniędzy, i danych konta bankowego.

Punktem wyjścia niech będą bezpośrednie ataki na serwer. Pierwszy z nich to DOS. Jest atakiem na serwer poprzez zapchanie zasobów systemu banku, aby nikt nie mógł skorzystać ze strony internetowej. Kolejnym sposobem jest zastosowanie oprogramowania do włamania i korzystania z zasobów serwera banku. Zalicza się do nich bakterie, robaki, konie trojańskie oraz bomby logiczne. Pierwsze z nich to oprogramowanie służące do replikacji w celu zablokowania systemu. Robaki natomiast mają za zadanie przenoszenia się z systemu na system. W skład niego mogą wchodzić bakterie lub wirusy, które zostają na zainfekowanym urządzeniu. Specyficznym programem jest koń trojański. Jego zadaniem jest udawanie innego oprogramowania i z ukrycia naruszanie systemu bezpieczeństwa sprzętu. Natomiast bomby logiczne to nieudokumentowane fragmenty programu, uruchamiające się w ustalonym czasie lub w ramach konkretnego

[7] K. Korzeń, *Bankowość elektroniczna jako kanał dystrybucji usług bankowych,* Poznań 2007, s. 71.

zdarzenia. Kolejnym sposobem włamania do systemu jest wykorzystanie furtek, czyli ukrytych wejść do legalnego oprogramowania, pozwalające na ominięcie zabezpieczeń. Dochodzi również do bezpośrednich ataków na bazy danych banków. Poważnym problemem jest nielojalność, co za tym idzie nieuczciwość pracowników oraz ich wszelakie błędy i przeoczenia. Do nich zaliczamy również cyberterroryzm i sabotaż komputerowy. Ostatnim ważnym zagrożeniem, są sytuacje nie związane bezpośrednio z działaniem systemu, to wszelakie zdarzenia losowe na przykład powodzie, pożary, awarie zasilania, wyładowania atmosferyczne i temu podobne[8]. W obszarze kradzieży danych bankowych, można wymienić poniższe przykłady. Pierwszym z nich jest tak zwany *skimming*. Polega na zainstalowaniu na bankomacie specjalnego urządzenia które pozwala na kopiowanie danych z karty bankowej. Wyglądem przypomina cześć składową bankomatu. W ten sposób przestępcy mogą wykonać duplikat karty lub zebrane dane przesłać dalej, tak aby inna osoba mogła wykonać kopię tej karty. Sposobem na niedopuszczenie do tego jest mechanizm wibrujący, niepozwalający na tą operacje kopiowania danych z kart. Jednak, aby skorzystać z tej kopii przestępca potrzebuje kod do karty. W tym przypadku stosowane są listwy z zamontowaną małą kamerką lub fałszywe klawiatury montowane na prawdziwej. W ten sposób złodziej dowiaduje się o kodzie PIN. Wybierane do *skimmingu* są bankomaty zlokalizowane tam gdzie przebywa dużo osób, takie jak np. szlaki turystyczne. Zwykle te urządzenia noszą ślady użytkowania, przez to nie zwraca się uwagi na szczególną ingerencje w nie, ani na obecność ludzi wokół niego. W celu zabezpieczenia dodatkowo instaluje się chip, który nie da się skopiować. Bez tego chipu nie ma możliwości wykorzystania skopiowanej karty, gdyż bankomaty w Polsce wymagają sprawdzenia tego chipu. Jednak nie daje to pełnej ochrony, gdyż są kraje na świecie, gdzie owej technologii się nie stosuje, co pozwala na wykorzystanie odtworzonych tą metodą kart. Kolejną metodą jest wszelakie wyłudzenie danych umożliwiające wykonanie transakcji. W tym celu przestępcy mogą zadzwonić do ofiary podając się za obsługę banku i wymusić na niej podanie danych do konta bankowego pod różnymi pretekstami na przykład w ramach sprawdzenia bezpieczeństwa. Innym

[8] A. Gospodarowicz, *Bankowość...*, s. 75-76.

tego typu sposobem jest wysłanie osobom wiadomość e-mailową która do złudzenia przypomina tę otrzymywaną z banku. Często zawiera ona odnośnik do strony internetowej. Owa strona też jest specjalnie spreparowana, tak aby przypominała stronę banku. Osoba, która się tam zaloguje przekazuje przestępcom dane potrzebne do logowania. Ten rodzaj przestępczości nazywamy *phishingiem*. Również ten sposób można wykorzystać do zainfekowania komputera, co w konsekwencji może doprowadzić do ataku na komputer klienta banku. Kolejnym zagrożeniem jest kradzież kart zbliżeniowych. Złodziej może wykorzystać brak wymogu podaniu kodu PIN do kwoty pięćdziesięciu złotych lub wykorzystać jej do płatności w której karta nie jest potrzebna na przykład przez internet[9]. Można również skorzystać ze spisania danych karty zbliżeniowej ze specjalnej aplikacji pozwalającej na ich zgranie. Wystarczy zbliżyć telefon z włączoną aplikacją do karty. Aplikacja nie pobiera kodu CVC2/CVV2 potrzebnego do zrealizowania transakcji w Polsce jak i w krajach europejskich[10]. Kolejnym zagrożeniem jest niewiedza dotycząca zagrożenia spowodowanego udostępnianiem wyglądu swojej karty na stronach społecznościowych, co w efekcie prowadzi do utraty środków pieniężnych na tym koncie. Wszelkie informacje, które są podawane w internecie zostają tam na zawsze. Aby wykorzystać dane z karty wystarczy jej przednia część. Podobnie jak w poprzednich przypadkach mimo nie posiadania kodu CVC/CVV2, przestępca może uzyskane dane wykorzystać na stronach w krajach w których owe zabezpieczenie nie jest wymagane. Dane takie jak numer karty, data ważności, imię i nazwisko posiadacza wystarczą do zawarcia transakcji. Kolejnym sposobem na kradzież pieniędzy na koncie bankowym jest wykorzystanie płatności mobilnych. Polega na kradzieży *smartphona* i dzięki niej złodziej pobiera środki zastane na koncie bankowym. Ułatwieniem w tym jest pozostawienie kodu potrzebnego do zalogowania w telefonie. Kolejnym zagrożeniem jest kradzież tożsamości. Polega na wykorzystaniu danych osobowych innej osoby w celu zaciągnięcia kredytu bankowego.

---

[9] M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną,* Warszawa 2014, s. 9-16.

[10] http://tech.wp.pl/kat,130058,title,Jak-ukrasc-dane-karty-platniczej-przy-pomocy-smartfonu,wid,14704314,wiadomosc.html?ticaid=116dbe (dostęp 03.05.2016).

Można zdobyć te dane poprzez rozmowę telefoniczną lub podszywanie się pod pracodawcę poszukującego pracownika i proszącego o wypełnienie obszernego kwestionariusza. Następną metodą na wyłudzenie pieniędzy jest „oszustwa nigeryjskie". Polega na wysłaniu wiadomości drogą elektroniczną, podając się za księcia jakiegoś kraju afrykańskiego z prośbą o pomoc w ukryciu majątku króla przed dyktaturą wojskową poprzez wysłanie środków na podane konto bankowe. Za przelanie tych środków, ofiara miałaby otrzymać procent od przelanej kwoty. Efektem tego jest tylko utrata środków, które znajdowały na podanym koncie. Występuje również ryzyko, że ta wiadomość może zawierać szkodliwe oprogramowanie. Ostatnim zagrożeniem są kradzieże w sklepach internetowych, aukcje internetowe i tym podobne. Funkcjonują one na zasadzie zamieszczenia ogłoszenia z ciekawym produktem o bardzo atrakcyjnej cenie, która jest nawet niższa od ceny rynkowej. Ofiara zainteresowana ofertą, dokonuje zakupu i wysyła przelew na konto. Jednak efektem nie jest dostanie owego produktu, a tylko utrata środków na koncie bankowym[11]. Poniżej zostaną przedstawione przykładowe włamania, np. oszustwa jakie można napotkać podczas użytkowania. W marcu 2016 roku ofiarą hakerów został bank centralny Bangladeszu. Oszuści dokonali kradzieży na kwotę 81 milionów dolarów[12]. Kolejnym przykładem jest niebezpieczne oprogramowanie, który infekuje telefony z systemem Android. Nazywa się GM Bot. Potrafi między innymi czytać jak i rozsyłać wiadomości SMS oraz przekazywać połączenia i tym podobne[13].

1.4. Zasady bezpiecznego korzystania z bankowości elektronicznej

Przedstawione zostaną tutaj zasady prawidłowego korzystania z usług bankowych. Pierwszą najważniejszą zasadą jest łączenie się bankiem za pomocą urządzeń, do których mamy zaufanie. Komputer do którego dostęp

[11] M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe...*, s. 16- 22.

[12] http://wyborcza.biz/biznes/1,147883,19772174,hakerzy-ukradli-80-mln-dol-banku-centralnego-bangladeszu-prezes.html#BoxBizImg (dostęp 03.05.2016).

[13] http://technowinki.onet.pl/oprogramowanie/mbank-ostrzega-uzytkownikow-telefonow-z-systemem-android/rs00t7 (dostęp 03.05.2016).

ma dużo osób, może być zainfekowany wirusami potrafiącymi skraść dane potrzebne do wykonania operacji na koncie bankowym. Kolejną zasadą jest sprawdzanie stron internetowych, czy zaczynaj się od https:// i czy strona szyfruje dane. Następną zasadą jest nie odpowiadanie na wiadomości, proszące o weryfikowanie danych bankowych, gdyż bank nie prosi cię o podanie danych poufnych. Ważną zasadą jest instalowanie oprogramowania na komputerze czy *smartfonie*, tylko z zaufanych źródeł. Nie należy również trzymać informacji potrzebnych do wykonywania operacji bankowych przy urządzeniu oraz również ich nie należy udostępniać osobom trzecim. Kolejna zasadą jest aktualizowanie systemu operacyjnego jak i oprogramowania co pozwoli na zniwelowanie ryzyka włamania do nich. Ostatnią równie ważną zasadą jest wylogowanie się z konta bankowego po zakończonej pracy[14].

1.5. Zakończenie

Zebrane tutaj informacje pokazują, że rozwój bankowości elektronicznej pozwala na przyjemniejsze i szybsze korzystanie z usług bankowych, ale dzięki nim możliwa staje się kradzież środków z kont bankowych. Jednakże ciągle rozwijane systemy chroniące operacje skutecznie nie pozwalają na kradzież pieniędzy. Należy pamiętać również o tym, że o bezpieczeństwo operacji należy zadbać osobiście.

Bibliografia

A. Matuszyk, P.G. Matuszyk, *Instrumenty bankowości elektronicznej*, Wydawnictwo CeDeWu sp. z o.o., Warszawa, 2011.

A. Gospodarowicz, *Bankowość elektroniczna,* Polskie Wydawnictwo Ekonomiczne, Warszawa 2005.

K. Korzeń, *Bankowość elektroniczna jako kanał dystrybucji usług bankowych,* Integraf-Anna Dygas , Poznań 2007.

[14] http://www.bsjaroslaw.pl/aktualnosci/id74,Zasady-bezpiecznego-korzystania-z-bankowosci-internetowej.html (dostęp 03.05.2016).

M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną,* Urząd Komisji Nadzoru Finansowego Warszawa 2014.
http://home.agh.edu.pl/~woznicki/tokeny.html.
http://tech.wp.pl/kat,130058,title,Jak-ukrasc-dane-karty-platniczej-przy-pomocy-smartfonu,wid,14704314,wiadomosc.html?ticaid=116dbe.
http://wyborcza.biz/biznes/1,147883,19772174,hakerzy-ukradli-80-mln-dol-banku-centralnego-bangladeszu-prezes.html#BoxBizImg.
http://technowinki.onet.pl/oprogramowanie/mbank-ostrzega-uzytkownikow-telefonow-z-systemem-android/rs00t7.