Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

Łukasz Zakonnik

Uniwersytet Łódzki
Wydział Ekonomiczno-Socjologiczny
Katedra Informatyki Ekonomicznej
lukasz.zakonnik@uni.lodz.pl

Przemysław Dembowski

Uniwersytet Łódzki
Wydział Zarządzania
Katedra Informatyki
pdembowski@wzmail.uni.lodz.pl

BEZPIECZEŃSTWO BANKOWOŚCI INTERNETOWEJ W POLSCE NA PRZESTRZENI LAT 2002-2017 – PRZEGLĄD ROZWIĄZAŃ OFEROWANYCH KLIENTOM INDYWIDUALNYM

Streszczenie: W artykule autorzy opisują metody mające zapewnić bezpieczeństwo w bankowości internetowej z punktu widzenia klienta indywidualnego w Polsce. Przedstawiono aspekt szyfrowania komunikacji, a także proste, złożone oraz dodatkowe metody uwierzytelnienia. W artykule dokonano przeglądu metod stosowanych w ciągu ostatnich 15 lat (do roku 2017). Zwrócono uwagę na metody, które stosuje się coraz rzadziej (tokeny) oraz na te najbardziej aktualne (kody SMS).

Słowa kluczowe: bankowość internetowa, bezpieczeństwo, uwierzytelnienie.

JEL Classification: G21.

Wprowadzenie

Bezpieczeństwo korzystania z Internetu od wielu lat jest przedmiotem analiz dokonywanych przez wielu specjalistów. Niemniej większość użytkowników kwestie bezpieczeństwa zaczynają interesować dopiero wtedy, kiedy zdadzą sobie sprawę, że narażeni są na utratę własnych środków pieniężnych. Przedstawiany artykuł ma odpowiedzieć na pytanie, czy korzystanie z bankowości internetowej jest bezpieczne – na jakie metody zabezpieczeń powinien zwrócić uwagę zwykły użytkownik i jak stosowane metody zmieniały się na przestrzeni ostatnich 15 lat (do roku 2017). W polskiej literaturze przedmiotu można odna-

leźć wiele analiz dotyczących poruszanego zagadnienia[1], jednak przedstawiany artykuł – obok czysto technicznego omówienia metod – dokonuje przeglądu zmian, jakie nastąpiły w analizowanych rozwiązaniach (z punktu widzenia klienta) od początku funkcjonowania bankowości internetowej w Polsce.

1. Bezpieczeństwo jako czynnik decydujący o rozwoju bankowości internetowej

Bankowość internetowa ma już stosunkowo długą historię. Pierwszym bankiem oferującym klientom usługę dostępu do swojego konta poprzez Internet był amerykański La Jolla Bank FSB [Zakonnik, 2002, s. 10]. Powstał on pod koniec 1994 r. Początkowo klienci banku, przy pomocy komputera podłączonego do Internetu, mogli jedynie sprawdzać stan swojego konta. Zaznaczyć jednak należy, że bank FSB posiadał rozbudowaną sieć placówek, tak więc oferowany dostęp do rachunku był praktycznie pewnym zabiegiem marketingowym i prostym rozwinięciem oferowanych funkcjonalności.

Inaczej sprawa wyglądała w przypadku amerykańskiego Security First Network Bank (SFNB) – rozpoczął on swoją działalność 18 października 1995 r. Był to pierwszy bank, który można było nazwać bankiem internetowym[2]. Jeden z twórców banku chciał wykazać zalety swojego produktu – bezpiecznego systemu operacyjnego SecureWare. Połącznie wiedzy bankowej ze znajomością technik bezpieczeństwa okazało się czynnikiem kluczowym i w efekcie stało się kamieniem milowym na drodze rozwoju nowych metod dostępu do usług bankowych. Pomimo zaciekawienia, jakie wywołało pojawienie się SFNB na rynku, niewielu specjalistów wróżył sukces całemu przedsięwzięciu. Jednakże już w trakcie pierwszego miesiąca działalności bank zdobył 1000 klientów (poza podkreśleniem bezpieczeństwa głównym magnesem okazały się także niskie opłaty i wysokie oprocentowanie możliwe dzięki redukcji kosztów funkcjonowania banku nowego typu). Warto dodać, że po sukcesie SFNB zaczęto próbować tworzyć jeszcze bardziej innowacyjne rozwiązania – czego efektem były banki wirtualne[3].

---

[1] Wśród pozycji książkowych np.: [Grzechnik, 2000; Koźliński, 2004; Chmielarz, 2005; Wawrzyniak, 2005; Świecka, 2007].

[2] Bank internetowy to: „przedsiębiorstwo bankowe nie mające innych kanałów dystrybucji poza Internetem (a w szczególności sieci oddziałów), względnie takie, w którym te kanały odgrywają marginalną rolę" [Grzechnik, 2000, s. 56].

[3] Bank wirtualny: „to bank, którego głównym zasobem jest marka i […] dobry serwis www. Sprzedawane za jego pośrednictwem produkty są w rzeczywistości produktami innych firm finansowych. Sam bank wirtualny jest więc właściwe swego rodzaju elektronicznym finansowym supermarketem […]" [Grzechnik, 2000, s. 56].

Pierwszym z tego typu banków był First-e, który zapewniał klientom pełną gamę produktów bankowych. Produkty te jednak nie były oferowane przez sam First-e. Bank korzystał po prostu z usług outsourcingowych innych instytucji finansowych – samemu dbając o funkcjonalną stronę WWW.

W przypadku Polski początki bankowości internetowej sięgają 1998 r. Chronologiczna lista banków oferujących usługi bankowości internetowej przedstawia się następująco:

1. PBG (Pekao SA.) – 10.1998.
2. Wielkopolski Bank Kredytowy (połączony z Bankiem Zachodnim) – 09.1999.
3. Bank Przemysłowo-Handlowy (połączony z Powszechnym Bankiem Kredytowym) – 11.1999.
4. Pierwszy Polsko-Amerykański Bank (później Fortis Bank, a w końcu w ramach BPH) – 01.2000.
5. Lukas Bank (Credit Agricole Bank Polski) – 03.2000.
6. Handlobank (Citibank Bank Handlowy) – 05.2000.
7. mBank – 11.2000.
8. PKO BP – 12.2000.
9. Bank Śląski (następnie ING BŚ) – 03.2001.
10. VW Bank Direct – 04.2001.
11. Inteligo (funkcjonuje oddzielnie, ale obecnie w ramach PKO BP) – 05.2001.
12. Bank Gospodarki Żywnościowej (następnie BGŻ BNP Paribas) – 07.2001.
13. LG Petrobank (następnie Nordea, w końcu przejęty przez PKO BP) – 07.2001.
14. Multibank (wchłonięty przez mBank) – 09.2001.
15. Nordea (przejęty przez PKO BP) – 11.2001.

Powyższą listę banków zakończono na tych, które z ofertą bankowości internetowej wystartowały do dnia 1 stycznia 2002 r.[4] (jak widać, większość dużych banków dokonała tego przed podaną datą). Należy zauważyć, że nie wszystkie wspomniane banki dotrwały w niezmienionej formie prawnej do dnia dzisiejszego. W efekcie końcowym do dalszej analizy wzięto pod uwagę jedynie 11 banków.

[4] Lista banków oferujących dostęp do rachunku przy pomocy Internetu rozrastała się praktycznie z miesiąca na miesiąc – np. można zauważyć, że ze swoją ofertą w lutym 2002 r. dołączył KredytBank.

2. Główne aspekty bezpieczeństwa bankowości internetowej z perspektywy klienta indywidualnego

Jak napisano to już w poprzednim punkcie – bezpieczeństwo dokonywanych operacji w bankowości internetowej jest jednym z głównych czynników decydujących o powodzeniu oferty wśród potencjalnych klientów.

2.1. Bezpieczeństwo komunikacji w ramach TCP/IP

Od czasu większej popularyzacji Internetu – a szczególnie od chwili, kiedy zaczęła się pojawiać możliwość realnego jego wykorzystania w biznesie – zaczęto zastanawiać się, jak zabezpieczyć popularne protokoły stosowane przez stos TCP/IP. Bez wątpienia największy sukces odniósł protokół rozwijany przez firmę Netscape – Secure Sockets Layer (SSL) i jego bezpośrednia modyfikacja – Transport Layer Security (TLS). Protokół ten, obok samego szyfrowania, zapewnił mechanizmy odpowiedniej weryfikacji i identyfikacji stron biorących udział w komunikacji. Dołączenie SSL (TLS) do HTTP zaowocowało dobrze znanym obecnie protokołem HTTPS, a klienci mogą rozpoznać bezpieczne połączenie poprzez symbol ikony z zamkniętą kłódką (symbol ten stosowany jest w wielu przeglądarkach internetowych). Warto jednak dodać, że o poziomie zapewnianego bezpieczeństwa nie decydowało jedynie zastosowanie konkretnego „szyfru", ale także długość zastosowanego klucza. Długość klucza, a tym samym jakość szyfrowania, podano w tabeli 1.

Tabela 1. Teoretyczna ocena bezpieczeństwa szyfrów symetrycznych w zależności od długości bitowej zastosowanego klucza

Długość klucza w bitach	Ocena bezpieczeństwa
40	Złamanie szyfru nie przysparza większych trudności
56	Złamanie szyfru jest trudne, ale leży w zasięgu zdeterminowanych podmiotów
64	Złamanie szyfru leży w zasięgu bardzo dużych organizacji
128	Teoretycznie odporne na złamanie w obecnej sytuacji
256	Odporne na złamanie w przewidywalnej przyszłości

Źródło: Opracowanie własne na podstawie: [Grzechnik, 2000, s. 109].

2.2. Pozostałe metody wpływające na bezpieczeństwo korzystania z bankowości internetowej[5]

Klient banku oferującego usługi bankowości internetowej, obok zabezpieczeń wynikających z użycia odpowiednich protokołów szyfrowania, powinien umiejętnie stosować cały szereg jeszcze innych metod podnoszących szeroko rozumiany poziom bezpieczeństwa dokonywanych operacji. Metody te mogą zadbać np. o prawidłowe uwierzytelnienie czy niezaprzeczalność wykonania danej operacji. Bardzo często wśród dodatkowych metod związanych z uwierzytelnieniem stosuje się podział na proste i silne (złożone) metody uwierzytelniające – opisane one zostaną w dalszej części artykułu.

2.2.1. Proste metody uwierzytelniające

Proste metody uwierzytelniające bazują głownie na tym, co klient (i zazwyczaj tylko on) powinien wiedzieć o własnym koncie (tzw. metody bazujące na tym „co się zna" [Wojciechowska-Filipek, 2011, s. 560]). Wśród tych informacji są zazwyczaj wymieniane:

1. Identyfikator – pewna, często skrótowa w stosunku do pełnego imienia i nazwiska nazwa jednoznacznie identyfikująca klienta.
2. Hasło – zazwyczaj ciąg liter, cyfr i znaków specjalnych, znanych tylko i włącznie klientowi. W praktyce można często spotkać się ze stosowaniem tzw. haseł maskowanych (bądź maskowalnych). Termin ten określa specyficzną technikę wprowadzania hasła do systemu, przy wykorzystaniu której nie podaje się wszystkich znaków hasła, a tylko te, o które poprosi system.
3. PIN – ciąg od 4 do 8 cyfr służący do potwierdzenia posiadania praw potrzebnych np. do użycia jakiegoś urządzania (np. odbezpieczenie tokenu).

Zazwyczaj w celu utrudnienia osobom niepowołanym odgadnięcia informacji (szczególnie hasła) tworzy się system zaleceń dbający o prawidłową konstrukcję i wykorzystanie tych danych. Polega to na tym, że np. hasło musi mieć określoną długość itd. Warto jednak pamiętać, że proste metody uwierzytelniające, bez metod dodatkowych, nie dostarczają wymaganego obecnie poziomu bezpieczeństwa.

[5] Zestaw metod – por. [Brakonicki, Dworakowski, Uryniuk, 2005, s. 17-18; Zalewska-Bochenko, 2013, s. 185-190].

2.2.2. Silne (złożone) metody uwierzytelniające

Drugą klasę metod stanowią silne (złożone) metody uwierzytelniające. Bazują one głownie na tym, co klient (i tylko on) powinien mieć (tzw. metody bazujące na tym „co się posiada" [Laskowski, 2008, s. 197]). Wśród tych unikalnych posiadanych „rzeczy" znajdują się przedmioty (np. karta elektroniczna, osobiste nośniki danych), na których umieszone są prywatne klucze używane w celu tworzenia podpisu cyfrowego (w sumie niezbyt często stosowane przez klienta indywidualnego ze względu na konieczność zapewniania dość drogiej infrastruktury). Spośród pozostałych „rzeczy" wyróżnia się:

a) tokeny,
b) listy haseł jednorazowych,
c) kody transakcji przesyłane poprzez SMS-y,
d) aplikacje mobilne.

Tokeny zazwyczaj występować mogą w dwóch postaciach. Pierwszą z tych postaci jest małe urządzanie przypominające kalkulator z (lub bez) klawiaturą i wyświetlaczem. W urządzaniu zaimplementowany jest odpowiedni algorytm szyfrujący, który używa unikanego klucza klienta. Głównym zadaniem tokenu jest wygenerowanie oraz wyświetlanie unikalnego dla klienta i dokonywanej operacji kodu. Tak użyty token będzie jednoznacznie świadczył o tożsamości i intencjach użytkownika.

W podobnym celu wykorzystuje się listę haseł jednorazowych (często używany jest tu skrót TAN – po angielsku: *Transaction Authentication Number*). Tak jak w przypadku tokenu, zatwierdzenie przez system bankowy jakiejś konkretnej operacji następuje po podaniu przez użytkownika hasła z listy. W przypadku listy haseł jednorazowych występuje ona w 2 formach:

– wydruk haseł (hasła podane są jawnie, więc każdy, kto choćby na chwilę miał dostęp do listy, będzie mógł w sposób niespostrzeżony zrobić kopie i spróbować wykorzystać),
– karta zdrapka (hasła są ukryte pod formą zdrapki – użytkownik wie doskonale, czy kod został już zużyty lub czy ktoś nie próbował go podejrzeć).

Pewną formą połączenia działania tokenu oraz haseł jednorazowych jest kod przesyłany SMS-em. Kod jest formą potwierdzenia planowanej operacji tak ze strony klienta, jak i banku – jest także bardzo efektywny w użyciu (zakładając posiadanie przez klienta telefonu komórkowego).

Aplikacje mobilne same w sobie mogą całościowo zastąpić obsługę banku z wykorzystaniem klasycznej przeglądarki (a więc mamy tu przykład bankowości mobilnej, a nie internetowej), ale mogą także stanowić prostą formę tokenu

albo listy haseł jednorazowych (wiązać się to może jednak z dodatkowymi zagrożeniami i koniecznością stosowania innych form zabezpieczeń [Nowacka, Szewczyk-Jarocka, 2016, s. 66])[6].

2.2.3. Dodatkowe formy zabezpieczeń[7]

Często pojawiającą się formą zabezpieczeń jest obrazek bezpieczeństwa. Stosowanie tej metody jest dodatkową formą uwierzytelnienia się banku przed klientem. Obrazek jest wybierany przez klienta przy otwieraniu konta internetowego. Bank za każdym razem przeprowadzania pewnych operacji (choć najczęściej ma to miejsce w przypadku logowania) – wyświetla obrazek na stronie WWW banku. Jako że tylko klient wie, jaki obrazek wybrał – jeśli go widzi na stronie WWW, wie, że musi to być strona autentyczna.

3. Przegląd zabezpieczeń stosowanych w polskiej bankowości internetowej

W punkcie tym zostanie przedstawiony przegląd stosowanych zabezpieczeń – analiza ta zostanie dokonana na podstawie stanu faktycznego zaistniałego w trzech różnych moment w czasie w ciągu ostatnich 15 lat.

3.1. Przypadek pierwszy – stan na 1.01.2002

Pierwszy z rozważanych przypadków dotyczy pewnego umownego początku powszechnego stosowania bankowości internetowej w Polsce. Dane zostały przedstawione w tabeli 2.

---

[6] Analiza aplikacji mobilnych wykracza jednak poza zakres tego artykułu; por. np. inny artykuł autora [Niewiadomski, Zakonnik, 2017, s. 161-177].

[7] Nie można zapominać o całym spektrum innych form zabezpieczeń – chociażby sprzętu klienta – poprzez stosowanie np. programów antywirusowych, firewalli, odpowiednich schematów zachowań (np. nieotwieranie nieznanych załączników poczty, nieznanych łączy internetowych) itd., por. [Parys, 2005, s. 221-224; Bandera, Grzywacz, 2016, s. 161-166]. Niemniej tego typu rozważania wykraczają poza ramy niniejszego artykułu.

Tabela 2. Wybrane formy zabezpieczeń stosowane przy obsłudze konta przez kanał WWW w wybranych bankach – stan na dzień 1.02.2002 r.

Nazwa banku (skrót)	Długość klucza	Proste uwierzytelnienie	Silne (złożone) uwierzytelnienie	Inne stosowane metody
BGŻ	128	identyfikator, hasło	token digipass	–
BPH PBK	128	identyfikator, hasło	podpis cyfrowy rsa	hasło maskowane
BZ WBK	128	identyfikator, hasło	token digipass	–
Handlobank (Bank Handlowy Citibank)	128	identyfikator, hasło (tzw. i-PIN)	–	–
ING	128	identyfikator, hasło	podpis cyfrowy rsa	hasło maskowane
Inteligo	128	identyfikator, hasło	lista haseł jednorazowych	–
Lukas (Credit Agricole)	128	identyfikator, hasło	token secureid	–
mBank	128	identyfikator, hasło	lista haseł jednorazowych	–
Pekao	128	identyfikator, hasło	token digipass	–
PKO	128	identyfikator, hasło	token activecard	–
VW Bank	128	identyfikator, hasło	token secureid	–

Źródło: Zakonnik [2002, s. 79-80].

Jak widać to na podstawie tabeli 2, wszystkie analizowane banki stosowały identyczną długość klucza (128 bitów – w ramach protokołu SSL). W związku z powyższym, jak sugerują to informacje zawarte w tabeli 1, działanie takie zapewniało (i to już 15 lat wstecz) bardzo dobry poziom szyfrowania, a tym samym bezpieczeństwa. W ramach prostego uwierzytelniania wszystkie banki stosowały identyfikator i hasło, z tą uwagą, że 2 banki (BPH oraz ING) dodatkowo używały haseł maskowanych (co jak wspomniano, uważane jest za podnoszące poziom bezpieczeństwa), niemniej 1 bank (Handlobank – później Citibank) stosował i-PIN (co z kolei uważać należało za pewną słabość – szczególnie zważywszy na niestosowanie silnych uwierzytelnień w tym banku). Praktycznie wszystkie banki (poza wspomnianym Handlobankiem) w celu dodatkowego zabezpieczenia oferowały albo token (w większości), albo listę haseł jednorazowych, ewentualnie podpis cyfrowy (po 2 banki). Biorąc pod uwagę przedstawione dane, widać więc, że już na początku funkcjonowania polskiej bankowości internetowej stawiano na mocne szyfrowanie i dodatkowe formy uwierzytelnienia (najczęściej realizowane przy wykorzystaniu tokenów). Stosowanie tokenów sprzętowych było jednak dość uciążliwe i mogło skutecznie uniemożliwić wykonywanie operacji np. poza domem (jeśli użytkownik akurat zapomniał tokenu). To przywiązanie klienta do jednego komputera pogłębiało wykorzystywanie niekiedy podpisów cyfrowych, w przypadku których należało zapewnić np. czytnik karty (ewentualnie plik z zainstalowanym certyfikatem).

Niedużą popularnością cieszyły się także karty haseł jednorazowych (często jeszcze nie w postaci zdrapki, ale prostej karty z wydrukiem haseł).

3.2. Przypadek drugi – stan na 1.09.2009

Jako drugi punkt w czasie przyjęto punkt pośredni w okresie minionych 15 lat. Odpowiednie dane zaprezentowano w tabeli 3.

Tabela 3. Wybrane formy zabezpieczeń stosowane przy obsłudze konta przez kanał WWW w wybranych bankach – stan na dzień 1.09.2009 r.

Nazwa banku (skrót)	Proste uwierzytelnienie	Silne (złożone) uwierzytelnienie	Inne stosowane metody
BGŻ	identyfikator, hasło	token sprzętowy (czas)	obrazek
BPH PBK	identyfikator, hasło	kody SMS, podpis elektroniczny sprzętowy	hasło maskowane
BZ WBK	identyfikator, hasło	kody SMS	obrazek
Bank Handlowy Citibank	identyfikator, hasło	kody SMS	–
ING	identyfikator, hasło	kody SMS	–
Inteligo	identyfikator, hasło	lista haseł jednorazowych	–
Lukas (Credit Agricole)	identyfikator, hasło	token sprzętowy (czas)	–
mBank	identyfikator, hasło	kody SMS	–
Pekao	identyfikator, hasło	kody SMS	hasło maskowane
PKO	identyfikator, hasło	lista haseł jednorazowych	–
VW Bank	identyfikator, hasło	token sprzętowy (czas)	–

Źródło: Macierzyński [2009, s. 11].

Po okresie 7 i pół roku analizie poddano wyłącznie wcześniej badane banki (których nazwa już czasami uległa zmianie). Niestety, zachowane dane nie zawierają informacji o długości klucza szyfrowania, ale w dużej mierze można założyć, że charakterystyka ta nie uległa zmianie. Podobnie stało się w przypadku prostego uwierzytelnienia (gdzie jedynie Bank Handlowy zrezygnował ze stosowania i-PIN-u). Doskonale widać natomiast powolne odchodzenie od tokenów (stosowały go powszechnie już tylko 3 banki). Rolę tokenów – w coraz szerszym zakresie – zaczęły przejmować kody przesyłane SMS-ami (postępowało tak już 6 banków). Lista haseł jednorazowych nadal była oferowana klientom, zanikać zaczęło natomiast szersze stosowanie podpisów cyfrowych (w formie sprzętowej). Pośród innych metod, do niezbyt jeszcze powszechnie stosowanych haseł maskowanych, dołączyły obrazki bezpieczeństwa.

3.3. Przypadek trzeci – stan na 1.01.2017

Jako ostatni analizowany stan wzięto pod uwagę początek bieżącego roku. Odpowiednie dane przedstawiono w tabeli 4.

Tabela 4. Wybrane formy zabezpieczeń stosowane przy obsłudze konta przez kanał WWW w wybranych bankach – stan na dzień 1.01.2017 r.

Nazwa banku (skrót)	Długość klucza	Proste uwierzytelnienie	Silne (złożone) uwierzytelnienie	Inne stosowane metody
BGŻ	256	identyfikator, hasło	kody SMS, podpis elektroniczny (sprzętowy)	hasło maskowane
BPH PBK	256	identyfikator, hasło	kody SMS	hasło maskowane
BZ WBK	256	identyfikator, hasło	kody SMS	obrazek, hasło maskowane
Bank Handlowy Citibank	256	identyfikator, hasło	kody SMS	–
ING	256	identyfikator, hasło	kody SMS	hasło maskowane
Inteligo	256	identyfikator, hasło	lista haseł jednorazowych TAN, kody SMS	obrazek
Lukas (Credit Agricole)	128	identyfikator, hasło	token sprzętowy (czas), SMSkody	–
mBank	256	identyfikator, hasło	kody SMS	–
Pekao	256	identyfikator, hasło	kody SMS, token sprzętowy	hasło maskowane
PKO	256	identyfikator, hasło	kody SMS, lista haseł jednorazowych	obrazek
VW Bank	256	identyfikator, hasło	kody SMS	hasło maskowane

Źródło: Opracowanie własne na podstawie informacji zawartych na stronach WWW poszczególnych banków.

W przypadku prezentowanej tabeli 4 widać jakościową zmianę w długości stosowanego klucza szyfrowania. Obecnie prawie wszystkie banki stosują klucz o długości 256 bitów (a więc uważany za niemożliwy do złamania w przeciągu przewidywalnej przyszłości), stosuje się także następcę protokołu SSL – TLS (w wersji 1.2). Wyjątkiem od wspomnianej reguły jest jedynie bank Credit Agricole stosujący TLS, ale z kluczem 128 bitowym (co jednak nie powinno wpłynąć na bezpieczeństwo komunikacji). Nie zmieniły się metody prostego uwierzytelniania, jednakże zaobserwować można częstsze stosowanie obrazków bezpieczeństwa i haseł maskowanych. W przypadku silnego uwierzytelniania każdy z banków – nawet jeśli wciąż oferuje inne rozwiązania – wykorzystuje kody SMS.

4. Uzyskane wyniki, krótkie porównanie ze światowymi trendami

Polska bankowość internetowa przeszła w ciągu ostatnich 15 lat dość długą drogę. Z usługi będącej swoistą ciekawostką stała się nieodzownym kanałem dystrybucji produktów bankowych dla ogromniej rzeszy klientów. Także i stosowane metody zabezpieczeń uległy – jeśli nie rewolucji – to widocznej ewolucji. O ile banki od samego początku zapewniały możliwie najlepszy sposób szyfrowania komunikacji (SSL i TLS o odpowiedniej, praktycznie najdłuższej możliwej wartości bitowej klucza), o tyle widać szeroki zakres zmian w zakresie stosowanych metod silnego uwierzytelnienia. Początkowo były to bezpieczne, ale mało wygodne w codziennym stosowaniu formy tokenów sprzętowych czy podpisów cyfrowych – obecnie mamy do czynienia z równie bezpiecznym (choć narażonym na inne rodzaje ataków) i bardziej elastycznym systemem weryfikacji z wykorzystaniem powszechnie dostępnych urządzeń mobilnych (telefony komórkowe i komunikacja SMS). Wydaje się, że powoli do przeszłości odchodzą listy haseł jednorazowych (jednak są wciąż oferowane – chociażby jako zabezpieczenie na wypadek awarii telefonii komórkowej). Widać także próby wprowadzania nowych rozwiązań, czego przykładem jest coraz częstsze stosowanie np. obrazków bezpieczeństwa. Sytuacja w bankowości w Polsce jest odbiciem trendów i rozwiązań dostępnych na rynkach światowych. Należy zauważyć, że stosowane rozwiązania w Polsce nie różnią się generalnie od najnowszych światowych standardów (np. wspomniane obrazki bezpieczeństwa czy hasła graficzne [Razvi i in., 2017, s. 35-41]), choć nie brak propozycji udoskonalania już istniejących metod (np. szyfrowanie krótkich wiadomości tekstowych SMS i użycie steganografii [Sheshasaayee, Sumathy, 2017, s. 709-717]). Zupełnie inną kwestią – wykraczającą poza ramy tego artykułu – staje się coraz częstsze postulowanie wprowadzania zupełnie nowych metod zabezpieczeń w bankowości mobilnej [Kiljan i in., 2017, s. 61:1-61:35].

Podsumowanie

Jako ostateczną konkluzję tego artkułu można przyjąć stwierdzenie, że bankowość internetowa jest z pewnością dość bezpieczną formą interakcji klient–bank, jednak coraz to nowe zagrożenia i pomysłowość przestępców z pewnością mobilizują banki do śledzenia zachodzących zmian, jak i stosowania nowych, skuteczniejszych sposobów podnoszenia bezpieczeństwa.

Literatura

Bandera R., Grzywacz J. (2016), *Zagrożenia bezpieczeństwa w bankowości elektronicznej*, „Zeszyty Naukowe PWSZ w Płocku, Nauki Ekonomiczne", t. XXIV, s. 151-168.

Brakonicki M., Dworakowski W., Uryniuk J. (2015), *Bezpieczeństwo bankowości elektronicznej* [w:] Materiały konferencyjne Mobile&Interent Banking Security, sierpień 2015, Obesrwatorium.BIZ, http://www.obserwatorium.biz/images/posts/raports/4_PL.pdf (dostęp: 29.11.2017).

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

Grzechnik J. (2000), *Bankowość internetowa*, Internetowe Centrum Promocji, Gdańsk.

Kiljan S., Simoens K., De Cock D., Van Eekelen M., Vranken H. (2017), *A Survey of Authentication and Communications Security in Online Banking*, "Journal ACM Computing Surveys", Vol. 49, Iss. 4, s. 61:1-61:35.

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

Laskowski P. (2008), *Bezpieczeństwo elektronicznych operacji bankowych*, "Scientific Bulletin of Chelm Section of Mathematics and Computer Science", No. 1, s. 193-201.

Macierzyński M. (2009), *Bezpieczeństwo w bankowości internetowej*, Raport Bankier.pl, https://www.bankier.pl/static/att/68000/2034334_raport102009.pdf (dostęp: 29.11. 2017).

Niewiadomski K., Zakonnik Ł. (2017), *Bankowość mobilna w Polsce – przegląd aplikacji, ranking, możliwości rozwoju*, „Przedsiębiorczość i Zarządzanie", t. XVIII, z. 4, cz. I, s. 161-177.

Nowacka A., Szewczyk-Jarocka M. (2016), *Bezpieczeństwo usług bankowości elektronicznej w opinii klientów banków spółdzielczych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", nr 307, s. 60-73.

Parys T. (2005), *Bezpieczeństwo transakcji bankowości internetowej z punktu widzenia klienta* [w:] *Systemy Wspomagania Organizacji SWO'2005*, Prace Naukowe, Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice, s. 219-225.

Razvi S.A., Neelima S., Prathyusha C., Yuvasree G., Ganga C., Kumar K.M. (2017), *Implementation of Graphical Passwords in Internet Banking for Enhanced Security* [w:] 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, Indie.

Sheshasaayee A., Sumathy D. (2017), *A Framework to Enhance Security for OTP SMS in E-Banking Environment Using Cryptography and Text Steganography* [w:] Proceedings of the International Conference on Data Engineering and Communication Technology, ICDECT 2016, Lavasa, Indie.

Świecka B. (2007), *Detaliczna bankowość elektroniczna*, CeDeWu, Warszawa.

Wawrzyniak D. (2005), *Bezpieczeństwo bankowości elektronicznej* [w:] A. Gospodarowicz (red.), *Bankowość elektroniczna*, PWE, Warszawa.

Wojciechowska-Filipek S. (2011), *Metody kontroli dostępu w bankowości elektronicznej* [w:] Konferencja Innowacje w Zarządzaniu i Inżynierii Produkcji, Zakopane.

Zakonnik Ł. (2002), *Przegląd i ocena ofert bankowości internetowej na rynku polskim*, praca magisterska, Uniwersytet Łódzki, Łódź.

Zalewska-Bochenko A. (2013), *Zabezpieczenie bankowych usług internetowych w Polsce* [w:] „Zeszyty Naukowe Uniwersytetu Szczecińskiego", nr 797, „Studia Informatica", nr 33, s. 181-194.

INTERNET BANKING SECURITY IN POLAND IN THE LAST 15 YEARS – A REVIEW OF THE SOLUTIONS OFFERED TO INDIVIDUAL CLIENTS

Summary: In the article, authors describe methods that provide security in Internet banking (from the perspective of an individual client in Poland). Authors presented the aspect of communication encryption, as well as simple, complex and additional authentication methods. This article reviews the methods used in the last 15 years. The authors describe the methods that are used less frequently (tokens) and the most popular (SMS codes).

Keywords: Internet banking, security, authentication.