PRACE NAUKOWE Akademii im. Jana Długosza w Częstochowie
Technika, Informatyka, Inżynieria Bezpieczeństwa 2016, t. IV, s. 147–162

http://dx.doi.org/10.16926/tiib.2016.04.12

Alina Gil, Krzysztof Senderecki
Wydział Matematyczno-Przyrodniczy
Akademia im. Jana Długosza w Częstochowie
al. Armii Krajowej 13/15, 42-200 Częstochowa
e-mail: a.gil@ajd.czest.pl

MECHANIZMY ZABEZPIECZANIA TRANSAKCJI ELEKTRONICZNYCH

Streszczenie. Transakcje elektroniczne, bankowość elektroniczna – to terminy, które na stałe zadomowiły się w naszym słownictwie. Bankowość elektroniczna jest formą kontaktu klienta z bankiem, pozwalającą na zdalną realizację usług bankowych za pomocą kanałów dystrybucji wykorzystujących technologie informacyjne, niewymagającą osobistego kontaktu i umożliwiającą sprawne zarządzanie finansami.
Zasadniczym czynnikiem rozwoju bankowości elektronicznej jest użyteczność i popularność wykorzystania internetowego kanału dystrybucji dóbr i usług.
Istotną barierą rozwoju bankowości elektronicznej jest zapewnienie bezpieczeństwa. Pomimo stosowania przez banki wielu metod zabezpieczeń danych klientów, a także przebiegu transakcji, nadal wiele osób powstrzymuje się od stosowania np. kart płatniczych, wykonywania przelewów czy płatności drogą elektroniczną, gdyż nie mają dość zaufania do tej formy.
Celem pracy jest analiza mechanizmów zabezpieczenia transakcji elektronicznych stosowanych przez banki jak również ukazanie środków kontroli dostępu do kont bankowych poszczególnych klientów. Przeprowadzono ponadto analizę raportów dotyczących bezpieczeństwa bankowości elektronicznej oraz systemów zabezpieczeń stosowanych przez banki.
Słowa kluczowe: bankowość elektroniczna, transakcje elektroniczne, uwierzytelnianie, autoryzacja, mechanizmy zabezpieczeń.

MECHANISMS FOR SECURING ELECTRONIC TRANSACTIONS

Abstract. Electronic transactions, e-banking - are terms, which permanently exists nowadays in our vocabulary. E-banking is a form of customer contact with the bank,

allows remote execution of banking services through distribution channels using information technology, does not require personal contact and enables efficient financial management.
The main factor in the development of e-banking is the usefulness and popularity of the use of the Internet distribution channel of goods and services.
A significant barrier to the development of electronic banking is to ensure safety. Despite the use by banks of many methods of security of customer data, as well as the course of the transaction, there are still many people which refrain from using Credit cards, making transfers and payments electronically, because they do not have enough confidence to this form.
The aim of the study is to analyze the mechanisms for securing electronic transactions used by banks as well as to present measures to control access to the bank accounts of individual customers. Moreover, the reports on the security of e-banking and security systems used by banks were analysed.
Keywords: e-banking, electronic transactions, authentication, authorization, security mechanisms.

Wprowadzenie

Podstawowym czynnikiem warunkującym rozwój usług bankowości elektronicznej są zagadnienia bezpieczeństwa transakcji elektronicznych.

Zapewnienie bezpieczeństwa nie jest działaniem jednorazowym, polegającym wyłącznie na wdrożeniu zabezpieczeń, ale na ciągłym, systematycznym nadzorze i przystosowywaniu do zmieniających się warunków otoczenia. Bezpieczeństwo należy rozpatrywać w aspekcie organizacyjnym, technicznym oraz prawnym. W poniższym artykule przedstawione zostaną zagadnienia związane głównie z aspektem organizacyjnym i technicznym. Rozwój technologii teleinformatycznych, coraz łatwiejszy dostęp do informacji oraz przetwarzania danych powoduje zwiększenie ryzyka naruszenia bezpieczeństwa procesów gromadzenia i wykorzystywania danych.

Bezpieczne świadczenie internetowych usług bankowych wymusza tworzenie systemów bezpieczeństwa związanych z identyfikacją klienta bankowego i autoryzacją składanych przez niego dyspozycji. Podstawowymi formami ochrony informacji w tych systemach są: szyfrowanie danych, system haseł, protokoły i algorytmy kryptograficzne oraz uwierzytelnianie użytkowników.

Szyfrowanie danych polega na przekształcaniu tekstu (jawnego) w ciąg znaków stanowiących szyfr. Proces ten jest realizowany przy użyciu algorytmu szyfrowania oraz specjalnego klucza szyfrującego. Odwrotnym procesem jest deszyfrowanie. System haseł dotyczy identyfikacji i potwierdzania tożsamości użytkownika w systemie komputerowym. System haseł jest niekiedy zastępowany metodami biometrycznymi lub uzupełniany dodatkowymi rozwiązaniami

typu: tokeny, listy haseł jednorazowych (potwierdzające każdą operację), karty chipowe, klucze sprzętowe i in. [5].

Dostęp do systemu informatycznego powinien być zabezpieczony za pomocą mechanizmów uwierzytelnienia, w którym każdy użytkownik ma przypisany jednoznaczny identyfikator oraz dane służące sprawdzeniu prawdziwości danych. Aby uzyskać dostęp do zabezpieczonego systemu, użytkownik musi wprowadzić swój kod i przypisane mu dane uwierzytelniające. Kontrolę dostępu otrzymuje się przez przypisanie w systemie konkretnemu użytkownikowi odpowiednich uprawnień, a także przez zapewnienie, że dane służące uwierzytelnieniu zna tylko użytkownik, którego one dotyczą.

Dostęp do informacji czy też funkcji służących wykonywaniu określonych operacji na danych jest przyznawany zgodnie z nadanymi dla konkretnego użytkownika uprawnieniami. Ponadto, wykonywane przez użytkownika operacje (w razie ich rejestrowania) powinny zwierać jego identyfikator [8].

Należy pamiętać, że identyfikator, hasło powinno być zmieniane, co jakiś czas i nie powinno być udostępniane. Stanowi ono swoisty elektroniczny podpis użytkownika. Hasło powinno zawierać co najmniej 6–8 znaków, nie tylko literowych, ale także liczbowych lub znaków specjalnych [2].

Bezpieczeństwo transakcji elektronicznych

Bankowość elektroniczną, ze względu na kanał komunikacji można podzielić na [1]:

- bankowość telefoniczną, w której kontakt klienta z bankiem następuje za pomocą telefonu (komórkowego, stacjonarnego),
- dedykowaną bankowość komputerową – komunikacja z bankiem odbywa się za pośrednictwem specjalnego oprogramowania i modemu,
- bankowość mobilną, z wykorzystaniem telefonów komórkowych,
- bankowość terminalową (samoobsługową) – dokonywanie transakcji przy pomocy elektronicznych urządzeń (bankomaty, terminale elektroniczne),
- bankowość internetową – dostęp do rachunku bankowego przy wykorzystaniu technologii przeglądarek internetowych.

Najczęstszą formą e-usług oferowaną przez banki są bankomaty, karty płatnicze, operacje bankowe dokonywane za pomocą telefonu lub Internetu.

W ujęciu informatycznym bezpieczeństwo to stan charakteryzujący się wysokim poziomem następujących atrybutów [4]:

- niezawodność – system działa w sposób bezawaryjny,
- poufność – tylko osoby uprawnione mają dostęp do przetwarzanych i przechowywanych w systemie danych,

- integralność – dane przesyłane w czasie transakcji nie są przez postronne osoby modyfikowane,
- niezaprzeczalność – nadawca nie może zaprzeczyć faktu nadania komunikatu,
- autentyczność – można stwierdzić, czy osoba podpisująca się pod dokonaną transakcją jest tą konkretną osobą,
- dostępność – stały dostęp do systemu bankowości, który jest oparty na dostępie do danych.

Analizując wskazane atrybuty bezpieczeństwa można wskazać potencjalne niebezpieczeństwa bankowości elektronicznej [3]:

- zagrożenie autentyczności – podrobienie,
- zagrożenie dostępności – przerwanie,
- zagrożenie integralności – modyfikacja,
- zagrożenie poufności – przechwycenie.

Barierą rozwoju bankowości elektronicznej są zagrożenia zewnętrzne, czyli włamania do systemu, nieuprawnione wykorzystanie kart magnetycznych, identyfikatorów, nieuprawnione ujawnienie danych, przechwycenie transakcji elektronicznych. Poniżej scharakteryzowano niektóre z nich [7]:

- Man-in-the-middle (człowiek pośrodku) – polega na modyfikacji i podsłuchu wiadomości przesyłanych pomiędzy dwiema stronami (bank-klient), bez ich wiedzy,
- Skimming – nielegalne skopiowanie paska magnetycznego karty płatniczej w celu stworzenia kopii lub wykonania niedozwolonej płatności za produkty i usługi, lub wypłaty z bankomatu. Wyróżnia się dwa typy skimmingu: bankomatowy oraz sklepowy.
- Man-in-the-broswer (człowiek w przeglądarce) – poprzez stosowanie złośliwego oprogramowania można dokonywać zmian w komputerze ofiary. Można przestawić poprawność certyfikatów, podsłuchać hasło, podmienić dane,
- Phishing (łowienie haseł) – dotyczy zmuszenia użytkownika do wejścia na fałszywa stronę, na której przestępca przechwytuje dane konieczne do autoryzacji. Może to być hasło, login użytkownika, czy lista kodów jednorazowych.

Zagrożenia związane ze świadczeniem usług bankowych wywołują u klientów obawę o bezpieczeństwo własnych środków finansowych i wpływają na obniżenie poziomu zaufania. Ogólną klasyfikację środków ochrony stosowanych przez banki przedstawia tabela 1.

Tab. 1. Klasyfikacja środków ochrony stosowanych w bankach

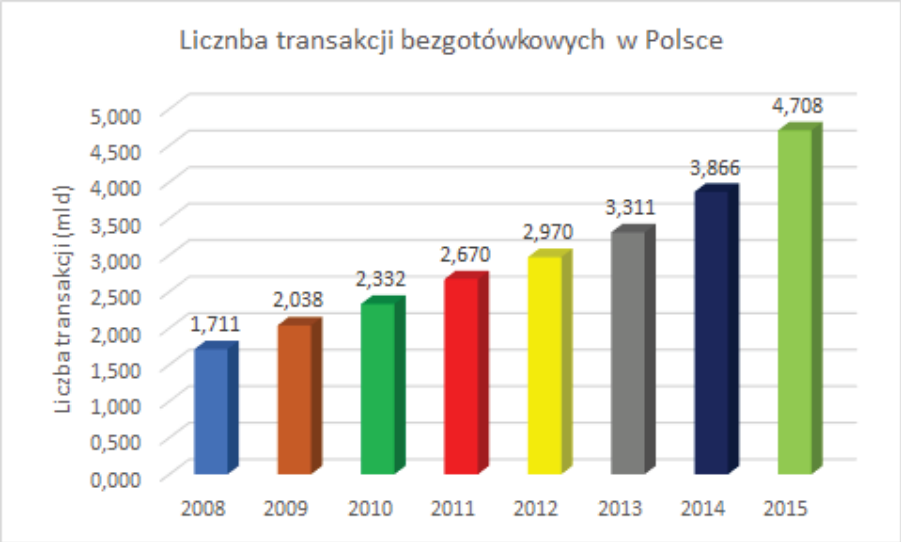
Kategoria	Charakterystyka zabezpieczenia
prawne	Unormowania prawne dotyczące ochrony danych przetwarzanych w bankach
techniczne	Rozwiązania sprzętowe: urządzenia podtrzymujące zasilanie, serwery Proxy, blokady dostępu do napędów dysku, klawiatur, urządzenie wykorzystywane do utworzenia kopii zapasowych wraz z metodami ich stosowania
fizyczne	Urządzenia antywłamaniowe, alarmy, sejfy
programowe	Rozwiązania zabezpieczające: programy śledzące, dzienniki systemowe, mechanizmy rozliczania, oprogramowanie antyspamowe, antywirusowe
kryptograficzne	Wysyłanie wiadomości w ukrytej postaci, tak aby odbiorca mógł ja odczytać
organizacyjne	Analiza ryzyka, polityka bezpieczeństwa
kontrola dostępu	Identyfikacja, autoryzacja, uwierzytelnienie

Źródło: Z. Mazur, T. Mendyk-Krajewska, *Bezpieczeństwo systemów informatycznych*, PTI, Katowice 2006, s. 35.

Nie sposób w jednym artykule zająć się wszystkimi kategoriami środków ochrony, dlatego w artykule omówione zostaną tylko niektóre.

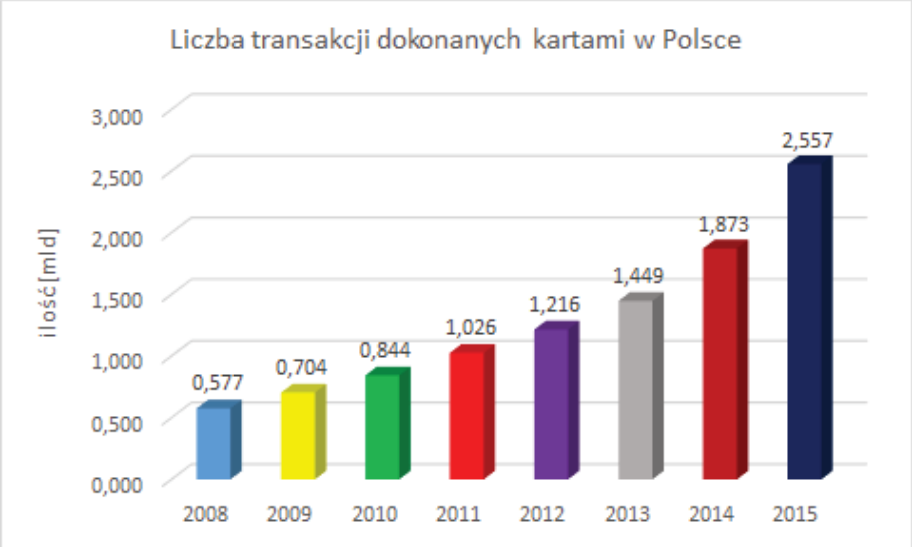
Zagrożenia instrumentów płatniczych

Jedną z najczęstszych form e-usług oferowanych przez banki są bezgotówkowe transakcje dokonywane przy pomocy kart płatniczych oraz operacji bankowych z użyciem telefonu lub Internetu. Na rysunku 1 przedstawiono liczbę transakcji bezgotówkowych dokonanych w Polsce w latach 2008–2015. W samym tylko 2015 r. liczba transakcji dokonanych kartą stanowiła 54,31%, natomiast przelewy – 45,13% ogólnej liczby transakcji bezgotówkowych.



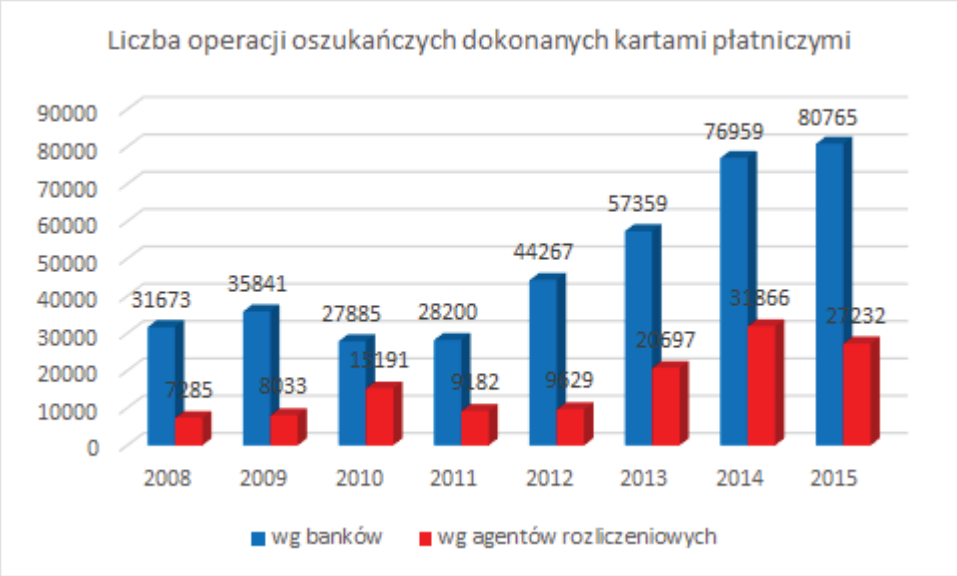
Rys. 1. Liczba transakcji bezgotówkowych w Polsce w latach 2008-2015 (sporządzono na podstawie danych z: Raportu NBP, *„Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2015”*, Departament Systemu Płatniczego, Warszawa 2016, s. 77)

Rysunek 2 przedstawia liczbę transakcji przeprowadzanych w Polsce przy użyciu kart płatniczych na przestrzeni ostatnich lat.



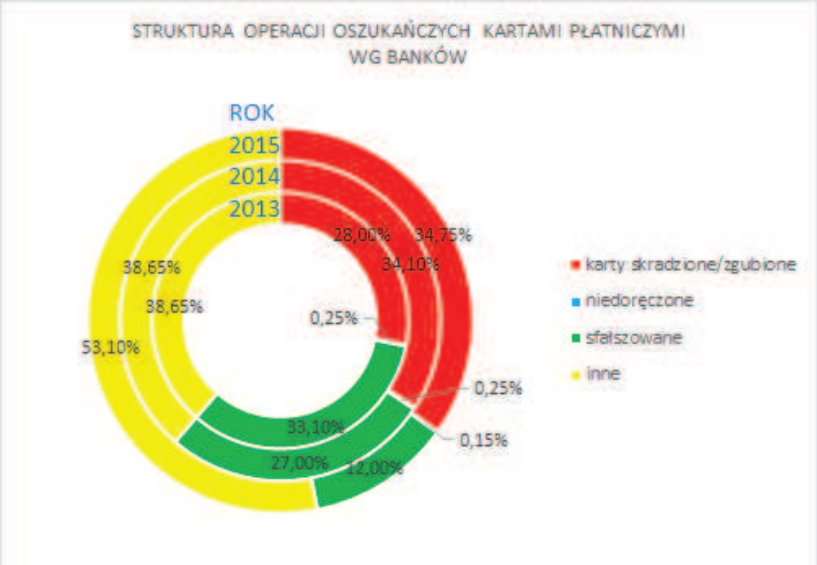
Rys. 2. Liczba transakcji dokonywanych kartami w Polsce w latach 2008-2015 (sporządzono na podstawie danych z: Raportu NBP, *„Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2015”*, Departament Systemu Płatniczego, Warszawa 2016, s. 77)

Rysunek 3 obrazuje liczbę transakcji oszukańczych dokonanych kartami płatniczymi w Polsce w latach 2008–2015. Liczba oszustw przekazywana przez agentów rozliczeniowych jest znacznie mniejsza od liczby przekazywanej przez banki. Dane od agentów rozliczeniowych nie obejmują transakcji dokonywanych przez oszustów w bankomatach kartami skradzionymi lub kartami skopiowanymi wraz z PIN-kodem oraz transakcji oszukańczych dokonanych poza granicami kraju kartami wydanymi w Polsce. Natomiast dane z banków nie obejmują bezgotówkowych transakcji oszukańczych dokonanych w Polsce kartami wydanymi w innych krajach [9].

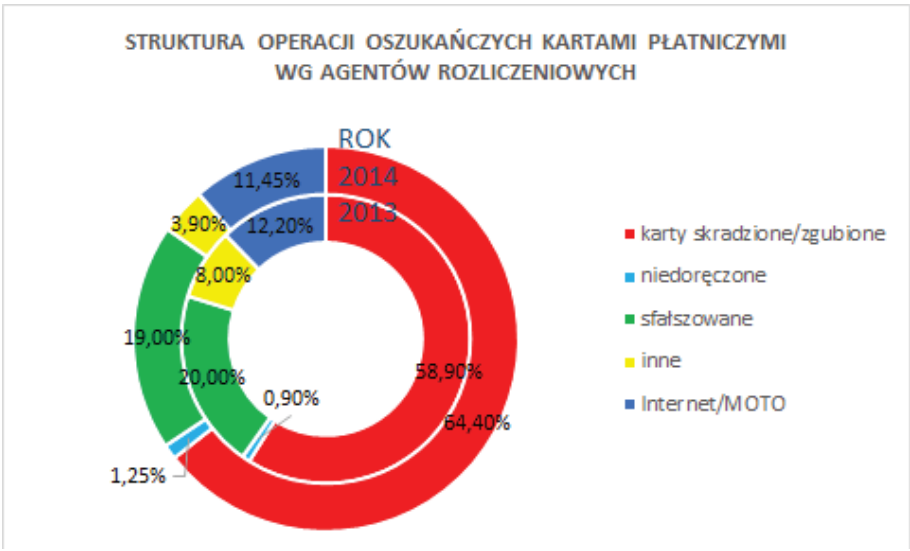


Rys. 3. Liczba transakcji oszukańczych z wykorzystaniem kart płatniczych w Polsce w latach 2008–2015 (sporządzono na podstawie danych z: Raportu NBP, *„Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2015”*, Departament Systemu Płatniczego, Warszawa 2016, s.89)

Strukturę operacji oszukańczych z wykorzystaniem kart płatniczych w Polsce w ostatnich latach z podziałem na rodzaje operacji oszukańczych przedstawiono na rysunkach 4 i 5.



Rys. 4. Struktura operacji oszukańczych z wykorzystaniem kart płatniczych w Polsce w latach 2013–2015 z podziałem na rodzaje operacji oszukańczych wg banków (sporządzono na podstawie danych z: Raportu NBP, „*Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2013, 2014, 2015*", Departament Systemu Płatniczego, Warszawa)



Rys. 5. Struktura operacji oszukańczych z wykorzystaniem kart płatniczych w Polsce w latach 2013–2014 z podziałem na rodzaje operacji oszukańczych wg agentów rozliczeniowych (sporządzono na podstawie danych z: Raportu NBP, „*Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2013, 2014*", Departament Systemu Płatniczego, Warszawa)

W analizowanym okresie największy udział oszustw kartowych, wg danych przekazanych przez banki, pod względem liczby transakcji wystąpił w transakcjach w kategorii Inne. Obserwowany jest spadek liczby i wartości transakcji oszukańczych dokonanych kartami sfałszowanymi.

Z danych otrzymanych od agentów rozliczeniowych liczba transakcji oszukańczych w II półroczu 2015 r. była wyższa niż w I półroczu, również wartość transakcji oszukańczych w II półroczu 2015 r. była wyższa niż w poprzednim. Według autorów raportu skala oszustw z użyciem kart jest niewielka w porównaniu do całości obrotu kartami płatniczymi.

Według ostatnich porównywalnych danych (za 2013 r.) Polska była na 3–4 miejscu w rankingu najbardziej bezpiecznych pod tym kątem krajów [9].

Uwierzytelnianie i autoryzacja w bankowości elektronicznej

Proces logowania do bankowości elektronicznej stanowi pierwszą przeszkodę przed nieautoryzowanym dostępem do informacji o rachunkach klienta i do jego środków finansowych. Metody uwierzytelniania klientów banków ciągle się zmieniają, powstają nowe regulacje, nowe koncepcje biznesowo-technologiczne, zmieniają się certyfikaty i szyfrowania połączeń.

Standardem jest otrzymanie przez klienta rozpoczynającego korzystanie z bankowości elektronicznej w danym banku tzw. „pakietu aktywacyjnego" zawierającego unikalny numer klienta, na początku najczęściej wspólny dla wszystkich kanałów dostępu oraz kod aktywacyjny, który umożliwia pierwsze logowanie do systemu a następnie powinien zostać zmieniony, aby stać się pełnoprawnym hasłem.

W bankowości internetowej czy mobilnej wprowadza się dodatkowe narzędzia mające na celu zwiększenie bezpieczeństwa korzystania z kanału np. hasła maskowane, kody SMS, tokeny, obrazki bezpieczeństwa (Tab. 2 i 3), jednak żadna z tych metod nie daje 100% zabezpieczenia i klient powinien zachować szczególną uwagę i skupienie przy procesie logowania.

Początkowo sposób logowania do kanału bankowości internetowej i mobilnej wyglądał podobnie, klienci korzystali z tych samych danych identyfikacyjnych, jednak ze względu na niewygodny proces logowania (przeniesienie rozwiązań z kanału internetowego w skali 1:1 do kanału mobilnego przy znacznie mniejszych rozmiarach ekranu) uproszczono logowanie – wprowadzono skrócone i uproszczone hasła, ale konieczne stało się przejście procesu rejestracji urządzenia mobilnego, czyli tzw. „dowiązanie" do kanału mobilnego w bankach.

Tab. 2. Narzędzia uwierzytelniania klienta w bankowości internetowej

	Bank	Alior	BZWBK	Eurobank	Getin	ING	mBank	Millenium	Pekao S.A.	PKO BP	Raiffeisen Polbank
Uwierzytelnianie - Internet	Własny Login	–	–	+	–	–	+	+	–	+	–
	Hasło maskowane	+	opcjonalnie	–	opcjonalnie	+	–	–	+	–	–
	Dodatkowe pytanie przy logowaniu	–	–	–	–	–	–	PESEL/ Paszport/ Dowód	–	–	–
	Obrazek bezpieczeństwa	+	opcjonalnie	–	–	–	–	opcjonalnie	–	–	–
	Dodatkowa autoryzacja (np. Kod SMS)	–	opcjonalnie	opcjonalnie	–	–	–	–	–	–	opcjonalnie

(Źródło: sporządzono na podstawie danych pozyskanych z: Raportu Specjalnego OBSERWATORIUM.BIZ „*Bezpieczeństwo bankowości elektronicznej*", 04/2015, s. 9).

Tab. 3. Narzędzia uwierzytelniania klienta w bankowości mobilnej

	Bank	Alior	BZWBK	Eurobank	Getin	ING	mBank	Millenium	Pekao S.A.	PKO BP	Raiffeisen Polbank
Uwierzytelnianie - mobilne	Konieczna aktywacja aplikacji	–	–	+	+	–	+	+	–	+	+
	Zapamiętywanie loginu	–	+	+	+	–	+	+	+	+	+
	Hasło maskowane	+	opcjonalnie	–	–	–	–	–	+	–	–
	Uproszczone hasło	–	opcjonalnie	+	+	+	+	+	–	+	+
	Logowanie biometryczne	–	–	–	–	–	–	+	–	–	–

(Źródło: sporządzono na podstawie danych pozyskanych z: Raportu Specjalnego OBSERWATORIUM.BIZ „*Bezpieczeństwo bankowości elektronicznej*", 04/2015, s. 10).

Podstawowym elementem ochrony danych i środków finansowych klientów bankowości elektronicznej są narzędzia autoryzacyjne, które mają chronić zarówno klienta, jak i instytucję finansową. Najbardziej popularne wśród narzędzi autoryzacyjnych stosowanych przez banki są kody SMS (Tab. 4 i 5), które jednak generują zbyt duże koszty i mogą być przejęte przez cyberprzestępców. Poszukiwania prostego substytutu dla kodów SMS doprowadziły do wprowadzenia tokenów mobilnych, które sprawdzają się bardziej w bankowości internetowej. Innymi stosowanymi metodami autoryzacji w bankach są tokeny sprzętowe (fizyczne) i listy kodów jednorazowych (zdrapki), lecz stanowią one jedynie narzędzie dla grupy klientów nie przekonanych do nowszych rozwiązań.

Tab. 4. Narzędzia autoryzacji transakcji w bankowości internetowej

	Bank	Alior	BZWBK	Eurobank	Getin	ING	mBank	Millenium	Pekao S.A.	PKO BP	Raiffeisen Polbank
autoryzacja - Internet	Kod SMS	+	+	+	+	+	+	+	+	+	+
	Token mobilny	–	–	+	–	–	–	–	+	+	–
	Token sprzętowy	–	–	–	–	–	–	–	+	–	–
	Autoryzacja przez serwis telefon.	–	–	–	–	+	–	–	–	–	–
	Autoryzacja zdrapką	–	–	–	+	–	+	–	+	+	+

(Źródło: sporządzono na podstawie danych pozyskanych z: Raportu Specjalnego OBSERWATORIUM.BIZ „*Bezpieczeństwo bankowości elektronicznej*", 04/2015, s. 11).

Tab. 5. Narzędzia autoryzacji transakcji w bankowości mobilnej

	Bank	Alior	BZWBK	Eurobank	Getin	ING	mBank	Millenium	Pekao S.A.	PKO BP	Raiffeisen Polbank
autoryzacja - mobilne	Brak autoryzacji do limitu wartości transakcji	–	+	–	–	+	–	–	–	w zależności od ustawień	+
	PIN mobilny	+	–	–	+	–	+	+	+	w zależności od ustawień	–
	Token mobilny	–	–	+	–	–	–	–	–	–	+
	Dzienny limit transakcji mobilnych	brak	+	+	+	+	+	+	+	w zależności od ustawień	+

(Źródło: sporządzono na podstawie danych pozyskanych z: Raportu Specjalnego OBSERWATORIUM.BIZ „*Bezpieczeństwo bankowości elektronicznej*", 04/2015, s. 13).

Autoryzacja transakcji w bankowości mobilnej jest znacznie bardziej skomplikowana, brakuje takiego standardu autoryzacji transakcji mobilnych jakim są kody sms w przypadku transakcji internetowych. Póki co, najważniejszym elementem zabezpieczenia aplikacji wszystkich badanych banków jest konieczność rejestracji urządzenia, na którym aplikacja bankowości mobilnej ma być zainstalowana. Rejestracja ta najczęściej wymaga kontaktu z serwisem telefonicznym lub wizyty w oddziale.

Autoryzacja transakcji w aplikacjach mobilnych wygląda bardzo różnie, jest realizowana poprzez zastosowanie limitów wartości transakcji, PIN-ów lub tokenów mobilnych lub określenie dziennych limitów transakcji mobilnych.

Tabela 6 przedstawia zestawienie najpopularniejszych narzędzi uwierzytelniania i autoryzacji z uwzględnieniem kanałów ich stosowania, kosztów dla instytucji finansowej, poziomu ryzyka i popularności wykorzystania przez banki.

Tab. 6. Zestawienie narzędzi uwierzytelniania i autoryzacji transakcji

	Kanał zastosowania	Koszt dla banku	Poziom ryzyka	Stosowanie przez polskie banki
Lista haseł jednorazowych	Internet Mobile - WEB Mobile - APP	Wdrożenie - średnie Utrzymanie - wysokie	Wysoki	Tak
Token mobilny	Internet Mobile - APP (lecz wówczas brak utrzymania standardu dwóch kanałów)	Wdrożenie - wysokie Utrzymanie - niskie	Niski w kanale Internet Średni w kanale Mobile	Tak (PKO - tylko do Internetu, Alior - również do Mobile z koniecznością osobnej instalacji, Raiffaisen Polbank - wbudowany w aplikację mobilną)
Token sprzętowy	Internet Mobile - WEB Mobile - APP	Wysoki (wydawnictwo i wymiana urządzeń)	Niski	Tak (głównie dla klientów firmowych)
Kod QR	Internet	Wdrożenie - wysokie Utrzymanie - niskie	Średni	Nie
Podpis elektroiczny	Internet	Wdrożenie - wysokie Utrzymanie - niskie	Niski	Rzadko (BGŻ BNP Paribas)

(Źródło: sporządzono na podstawie danych pozyskanych z: Raportu Specjalnego OBSERWATORIUM.BIZ „*Bezpieczeństwo bankowości elektronicznej*", 04/2015, s. 17).

Mechanizmy zabezpieczeń transakcji elektronicznych – kierunki rozwoju

Na polskim rynku został już wypracowany model zabezpieczania transakcji elektronicznych uwzgledniający specyfikę głównych kanałów dostępu do bankowości elektronicznej – internetowego i mobilnego, niemniej jednak przed sektorem finansowym wciąż stoi wiele wyzwań związanych z tworzeniem nowych zasad i narzędzi identyfikacji i uwierzytelniania.

Duże nadzieje związane z uwierzytelnianiem i autoryzacją transakcji w bankowości elektronicznej wiąże się z rozwojem narzędzi biometrycznych, które będą systematycznie standaryzowane, na przykład poprzez modele Fast Identity Online (FIDO). Techniki biometryczne zajmują się weryfikowaniem osób poprzez porównanie pewnych cech (odcisk palca, głos, twarz, oko) z zapisaną wcześniej próbką. Niestety metody biometryczne mają pewne wady np. nie u wszystkich osób dana cecha istnieje w stanie możliwym do pomiaru, ponadto prawie wszystkie cechy ulegają zmianie w trakcie życia. Ważne są też czynniki techniczne, a więc jakość odczytu parametrów biometrycznych, charakterystyka czujników, jakość połączenia.

Poszukiwania optymalnej i uniwersalnej metody autoryzacji dla bankowości mobilnej i internetowej prowadzone są np. w ramach tzw. USF (Universal Second Factor/Universal Authentication Framework) i mogą doprowadzić do wykorzystania rozwiązań sprzętowych na przykład „miksu" klasycznego tokena z urządzeniami typu „wearables", czyli tzw. urządzeniami ubieralnymi (smartwatche, inteligentne okulary, bransoletki, wirujące buty i in.).

W instytucjach finansowych musi nastąpić rozwój rozwiązań wewnętrznych, czyli procesów i systemów umiejących w elastyczny sposób odpowiedzieć na pojawiające się zagrożenia – wśród nich wymienić można: SIEM (Security Information and Event Management), SOC (Security Operation Center), systemy antyfraudowe „skanujące" ruch i transakcje w bankowości elektronicznej, czy międzyorganizacyjne systemy wymiany danych.

Bezpieczeństwo elektroniczne sektora finansowego, przy zwiększającej się popularności e-administracji, staje się interesem wagi państwowej, a nie tylko jednego z komercyjnych sektorów gospodarki.

Edukacja klienta jest również kluczowym elementem działań zabezpieczających zarówno banki, jak i samego klienta przed zagrożeniami i atakami cyberprzestępców.

Zasady bezpiecznego korzystania z bankowości elektronicznej obejmują zalecenia dla użytkowników dotyczące nawyków pewnych zachowań:

- nie podawać kodów, loginu, haseł, numerów telefonów na nieznanych stronach;
- aktualizować i zabezpieczyć komputer i telefon za pomocą programów antywirusowych;
- używać legalnego oprogramowania;
- właściwie wybierać, ustawiać i aktualizować przeglądarkę internetową;
- nie przechowywać informacji o szyfrowanych stronach (w tym celu stosować odpowiednie ustawienia pamięci podręcznej);
- sprawdzać certyfikaty bezpieczeństwa;
- chronić numer klienta i hasło, sprawdzać daty ostatniego logowania;
- logować się w zaufanych komputerach i sieciach, włączyć hasło do routera.

Do najnowszych zagrożeń dla bankowości elektronicznej należą:

- phishing mailowy sugerujący blokadę lub zmianę hasła internetowego;
- złośliwe oprogramowanie wyłudzające numer telefonu;
- maile phishingowe zawierające informacje o blokowaniu rachunku i konieczności odblokowania;
- nietypowe komunikaty na temat ubezpieczenia transakcji.

Należy uświadamiać klientów, aby nie podejmowali takich działań pożądanych przez przestępców.

Informowanie o zasadach bezpieczeństwa w serwisach mobilnych jest znacznie skromniejsze, wiele banków nie umieszcza żadnych informacji na ten

temat. Podstawowe zasady bezpiecznego korzystania z bankowości mobilnej to podstawowe zasady korzystania z telefonu komórkowego, a więc:

- aktualizacja oprogramowania systemowego;
- stosowanie zabezpieczeń – oprogramowania antywirusowego i zapory sieciowej;
- fizyczne zabezpieczenie telefonu – ochrona przed zgubieniem lub kradzieżą, uaktywnienie blokady dostępu do telefonu, niestosowanie łatwych PIN-ów, unikanie publicznych sieci Wi-Fi.

Podsumowanie

W XXI wieku odczuwamy coraz większe tempo zmian w zakresie bankowości elektronicznej. Coraz częściej mamy do czynienia z bankowością mobilną czy płatnościami zbliżeniowymi kartami, niebawem standardem staną się płatności telefonem.

Jak widać, wpływ innowacji IT na e-bankowość jest bardzo duży i dlatego tak ważne są działania podejmowane w zakresie bezpieczeństwa bankowości elektronicznej.

Komisja Nadzoru Finansowego wskazuje wytyczne w zakresie oceny ryzyka oraz polityki bezpieczeństwa płatności. Rekomendacje KNF oraz inne regulacje europejskie wskazują na potrzebę tworzenia nowych narzędzi zabezpieczania usług elektronicznych i to nie tylko tych widocznych dla klienta, ale i tych niewidocznych związanych z zabezpieczeniem systemów, monitorowaniem aktywności czy też wdrażaniem nowych rozwiązań technicznych po stronie banku czy instytucji płatniczej.

Na świecie działa wiele korporacji zajmujących się tematem bezpieczeństwem bankowości elektronicznej, takich jak RSA, IBM, CISCO, ale też pojawia się ogromna liczba dynamicznych firm, start-upów, które proponują ciekawe produkty. Wśród nich wymienić można:

- SecuRing, założona w 2003 roku, pracuje dla wiodących banków, ubezpieczycieli, telekomów, administracji publicznej i dostawców oprogramowania, dostarczając usługi, takie jak: testy bezpieczeństwa aplikacji i infrastruktury, definiowanie wymagań dotyczących bezpieczeństwa, szkolenia [11];
- Bit9, która w połączeniu z Carbon Black (www.redcanary.co) konkuruje z IBM w zakresie zabezpieczania urządzeń końcowych oraz serwerów w firmach na całym świecie;
- Norse (www.norse-corp.com), powstała w 2010 r. jest liderem w zakresie wykrywania ataków cyberprzestępczych;

– Fortscale, powstała w 2012 r., dostarcza technologię do budowy skalowanych rozwiązań analizy ryzyka dotyczącej aktywności użytkowników w firmie, w tym wizualizacji i raportowania [10].

Literatura

[1] Bajor B., (2011), *Bankowość elektroniczna*, Wyd. Scholar, Warszawa.
[2] Chrząszcz A., (2010), *Zabezpieczenie prywatności w usługach Internetowych*, Wyd. CERT Polska, Warszawa.
[3] Dmowski A., (2010), *Rynki finansowe*, Wyd. Digfin, Warszawa.
[4] Gospodarowicz A., (2006), *Bankowość elektroniczna*, PWE, Warszawa.
[5] Kolbusz E., (2005), *Inżynieria systemów informatycznych w e-gospodarce*, PWE, Warszawa.
[6] Mazur Z., Mendyk-Krajewska T., (2006), *Bezpieczeństwo systemów informatycznych*, PTI, Katowice.
[7] Patena W., Cwynar W., (2010), *Podręcznik do bankowości*, Oficyna a Wolters Kluwer business, Warszawa.
[8] Rudnicki A., (2007) *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów teleinformatycznych*, Wyd. Sejmowe, Warszawa.
[9] Raport NBP, *„Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2015”*, Departament Systemu Płatniczego, Warszawa 2016.
[10] Raport Specjalny OBSERWATORIUM.BIZ *„Bezpieczeństwo bankowości elektronicznej”*, 04/2015.
[11] https://www.securing.pl/index.html