• F I N A N S E I P R A W O F I N A N S O W E •
• Journal of Finance and Financial Law •

Numer specjalny/Special Issue 2/2022: 49–71

OCENA POZIOMU BEZPIECZEŃSTWA UŻYTKOWNIKÓW RACHUNKÓW BANKOWYCH I ANALIZA ZACHOWAŃ BANKÓW W SYTUACJI WYSTĄPIENIA INCYDENTU ZAGROŻENIA BEZPIECZEŃSTWA

Anna Popik[*], **Agnieszka Gryglicka**[**]

Member since 2021 JM15102

https://doi.org/10.18778/2391-6478.S2.2022.04

EVALUATING THE SECURITY OF ELECTRONIC BANKING IN USERS OPINION AND ANALYZING THE BEHAVIOR OF BANKS IN THE EVENT OF A SECURITY INCIDENT

Abstract

The purpose of this article. The aim of the article is to identify the opinions of bank customers on the level of security of electronic banking in Poland and to analyze the actions taken by banks in the event of a security incident.

Methodology. The analysis was based on data collected through a questionnaire survey. The survey with non-random sampling involved 222 people, and 217 records were included in the analysis. The form contained closed questions.

The result of the research. The analysis of the survey results indicates a high sense of security among bank account users, especially thanks to campaigns initiated by banks that inform customers about possible dangers. Respondents value direct communication and quick responses, which in this age of technological advances are the most important element in protecting customers. The literature review, which complements the survey, also confirms the high commitment of banking institutions in ensuring security. Despite the analysis of the survey results, it is important to bear in mind the lack of their translation to the general population, which does not allow a clear confirmation of the total security of customers holding funds in bank accounts.

Keywords: electronic banking, e-banking, security, cyber-security, banking fraud.

JEL Class: D18, G2.

[*] Mgr, Szkoła Doktorska Nauk Społecznych, Uniwersytet Warszawski, e-mail: a.popik@uw.edu.pl https://orcid.org/0000-0002-0979-3938

[**] Mgr, Szkoła Doktorska Nauk Społecznych, Uniwersytet Marii Curie-Skłodowskiej, e-mail: agnieszka.gryglicka@mail.umcs.pl http://orcid.org/0000-0003-0003-1600

WSTĘP

Posiadanie rachunku bankowego przez osobę dorosłą jest w dzisiejszych czasach działaniem niemal obligatoryjnym, zwłaszcza odkąd obrót bezgotówkowy cieszy się coraz większym zainteresowaniem. Cechujące się innowacyjnością technologie w obliczu wysokiej konkurencji w sektorze bankowym są podstawą i zarazem bodźcem dla tworzenia nowych produktów i usług bankowych, które ze względu na swój cyfrowy charakter dostępne są jedynie poprzez bankowość elektroniczną. Ta stała się jeszcze bardziej atrakcyjna w czasie pandemii COVID-19, kiedy zachęcano jej użytkowników do dokonywania płatności zbliżeniowych i zakupów online. Niestety, rachunki bankowe obarczone są ryzykiem związanym przede wszystkim z utratą ich bezpieczeństwa. W tradycyjnej formie przechowywania środków pieniężnych odpowiedzialność za pieniądze spoczywa na ich posiadaczu, co znacząco odróżnia ją od struktury funkcjonowania rachunków bankowych w elektronicznym kanale dystrybucji. W tym przypadku zapewnienie bezpieczeństwa kont bankowych nie leży jedynie po stronie klienta, a w dużej mierze zależy od samej instytucji bankowej. Powinien w niej bowiem istnieć i funkcjonować taki system zarządzania bezpieczeństwem, który działając w sposób sformalizowany identyfikuje i kontroluje ryzyko, skupiając się zwłaszcza na integracji przetwarzanych informacji (Rekomendacja D Komisji Nadzoru Finansowego, 2013).

Koniecznością staje się zatem opracowanie standardów i zachowań umożliwiających minimalizację zjawiska narażenia środków bankowych na jakiekolwiek niebezpieczeństwo. Kierując się tą potrzebą instytucje bankowe przekazują komunikaty i tworzą kampanie informujące o możliwych niepożądanych akcjach na rachunkach bankowych, które mogą stać się celem internetowych przestępstw. W dobie digitalizacji i przeniesienia wielu informacji w wirtualny świat jest to o tyle ważne, ponieważ obarczone ryzykiem nie muszą być jedynie pieniądze, ale też tożsamość i nowo powstałe zobowiązania, jakie z jej przechwycenia mogą wynikać.

Celem artykułu jest identyfikacja opinii użytkowników bankowości elektronicznej na temat poziomu bezpieczeństwa środków przechowywanych na rachunkach bankowych w Polsce. Dodatkowo przeprowadzono analizę działań podejmowanych przez banki w sytuacji wystąpienia incydentu bezpieczeństwa (w sytuacji wystąpienia zdarzeń powodujących wyciek danych osobowych czy wykorzystanie złośliwego oprogramowania do celów przejęcia środków z rachunków bankowych). Powołując się na dotychczasowe doświadczenia związane z bankowością elektroniczną i akty prawne, na podstawie których funkcjonują instytucje bankowe, sformułowano pytanie: Czy instytucje bankowe dbają o bezpieczeństwo rachunków bankowych swoich klientów z należytą starannością?

Bazując na dostępnej literaturze oraz danych statystycznych opisano i uporządkowano wiedzę na temat najpopularniejszych incydentów zagrożenia bądź

braku bezpieczeństwa w usługach bankowych. Następnie przedstawiono dane ilościowe dotyczące liczby rachunków indywidualnych, liczby zaobserwowanych incydentów bezpieczeństwa (publikowanych w raportach CERT Polska), a następnie przedstawiono wyniki badań własnych dotyczących poziomu bezpieczeństwa usług bankowych z perspektywy ich użytkowników oraz sformułowano wnioski.

1. BEZPIECZEŃSTWO USŁUG BANKOWYCH

Bankowość elektroniczna jest jednym z najszybciej rozwijających się segmentów rynku finansowego (Alansari i in., 2021: 845). Bankowość elektroniczna, nazywana również bankowością online, rewolucjonizuje branżę usług finansowych (szczególnie w zakresie obsługi produktów bankowych i realizacji usług z nimi związanych) przy użyciu zdalnych kanałów dostępu (Nosowski, 2005: 26; Melnychenko i in., 2020: 92), bez konieczności wizyty w banku bądź jego filii (Lenka i Barik, 2018: 2). Wpływa również na ostateczne wybory klientów banku w życiu codziennym, otwierając nowe możliwości zaspokajania ich potrzeb. Bankowość elektroniczną można podzielić na trzy główne obszary: bankowość internetową, mobilną oraz płatności z użyciem kart. Bankowość internetowa polega na wykorzystaniu komputera (stacjonarnego lub przenośnego – laptopa) lub urządzenia mobilnego. Bankowość mobilna polega na wykorzystaniu aplikacji bankowych zainstalowanych na urządzeniach mobilnych (smartfon, tablet). Płatności z użyciem kart rozwijają się dynamicznie, obejmują nie tylko transakcje płatnicze z wykorzystaniem kart płatniczych, ale też wykorzystanie technologii zbliżeniowej NFC (*Near Field Communication* – Komunikacja Bliskiego Zasięgu) przy użyciu aplikacji zainstalowanej w pamięci telefonu komórkowego (Krzysztoszek, 2017: 13). Wraz z rozwojem technologii i poszerzania wachlarza usług oferowanych przez instytucje finansowe pojawiają się nowe zagrożenia, zarówno dla klientów korzystających z tych rozwiązań, jak i samych instytucji (Jibril i in., 2020: 270).

Rozwój technologii internetowych, stron i aplikacji mobilnych pozytywnie wpłynął na jakość użytkowania serwisów, a tym samym satysfakcję i wygodę klientów instytucji finansowych (Moşteanu i in., 2020: 307–308). Niestety, spowodował również zwiększenie ryzyka zagrożenia bezpieczeństwa i prywatności (Liyanaarachchi i in., 2021: 955). Jednym z nich jest cyberprzestępczość (Alkahtani i in., 2020: 1–2).

Jeszcze dekadę wcześniej bankowość elektroniczna kojarzona była głównie ze sprawdzaniem stanu środków, zakładaniem lokat czy dokonywaniem przelewów. Aktualnie, zgodnie z art. 6 Ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. 2021, poz. 2439 z późn. zm.), posiadacz konta bankowego w Polsce, poza typowymi usługami bankowymi, może wykorzystać swoje konto w celu

założenia Profilu Zaufanego, załatwienia spraw urzędowych czy uzyskania dostępu do najważniejszych dokumentów potwierdzających tożsamość. Nieustannie poszerzający się zakres usług bankowych wiąże się z coraz większymi wymaganiami względem instytucji – z jednej strony konieczne jest zapewnienie bezpieczeństwa świadczonych usług, z drugiej natomiast skonstruowanie ich w taki sposób, aby były proste i przyjazne dla użytkowników.

Tabela 1. Występowanie incydentów zagrożenia bezpieczeństwa

	Liczba incydentów	
Rok	W sektorze bankowym	Ogółem
2018	643	3 739
2019	1 057	6 484
2020	1 008	10 420
2021	947	29 483

Źródło: opracowanie własne na podstawie raportów z działalności CERT Polska zawierających zebrane dane o zagrożeniach dla polskich użytkowników Internetu (www1).

Bezpieczeństwo jest jednym z głównych problemów związanych z bankowością internetową oraz szeroko pojętym *e-commerce* (handlem elektronicznym), dlatego stało się wręcz niezbędnym stosowanie narzędzi zabezpieczających przed różnego rodzaju cyberatakami, w celu zapewnienia bezpiecznej komunikacji pomiędzy systemem a szerokim wachlarzem usług oferowanych klientom (Omariba i in., 2012: 436–440).

Wśród aktualnie obowiązujących regulacji w prawie unijnym, mających na celu ochronę klientów banków przed niewłaściwym wykorzystaniem danych i maksymalizacją zysków ze strony dostawców usług finansowych wyróżniamy Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. nr 119, str. 1 z późn. zm.) oraz Dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego oraz Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (wersja przekształcona) (Dz.U. UE. L. z 2016 r. nr 26, str. 19 z późn. zm.) (IDD) (Freij, 2020: 181–190). Analizując przepisy, można zauważyć dążenie prawodawców w kierunku zwiększenia nacisku na bezpieczeństwo ekosystemów i interfejsów wykorzystywanych w oferowanych usługach finanso-

wych. Wzrasta również zapotrzebowanie na zwiększoną kontrolę firm, rozszerzenie wymogów sprawozdawczych, analizy KYC (*Know Your Customer* – zbiór informacji o kliencie umożliwiający ustalenie jego wiarygodności) oraz *due diligence* (należyta staranność, ocena aktualnej sytuacji przedsiębiorstwa i ryzyk z nim związanych), co tworzy kolejne ryzyko – niezachowania prywatności (Le Nguyen, 2018: 53–55).

Wprawdzie w aktualnym stanie prawnym w Polsce nie istnieje definicja bankowości elektronicznej (Lisowska i Waściński, 2021: 54), jednak można przyjąć, że jest to dostęp do zgromadzonych na rachunku bankowym środków finansowych wraz z towarzyszącymi im usługami, z wykorzystaniem stacjonarnych i mobilnych urządzeń elektronicznych. Regulacjami o największym zakresie przedmiotowym w kwestii bankowości elektronicznej w Polsce są przepisy ustawy Prawo bankowe (regulujące działalność banków) oraz ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. 2021, poz. 1907 z późn. zm.) (normujące relacje między bankiem a klientem).

Komisja Nadzoru Finansowego (dalej: KNF), jako organ nadzorczy, w swoich rekomendacjach (treść rekomendacji dostępna jest na stronie www.knf.gov.pl, wśród najistotniejszych należy wyróżnić Uchwałę Komisji Nadzoru Bankowego z dnia 11 grudnia 2002 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki oraz Uchwałę nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz.Urz. KNF z 2013 r. poz. 5)) przekazuje zalecenia dotyczące bezpieczeństwa płatności elektronicznych, wskazując pewne wytyczne oceny ryzyka i polityki bezpieczeństwa płatności. Rekomendacje służą przypomnieniu dobrych praktyk i standardów, jakimi instytucje finansowe powinny się kierować podczas przeprowadzania audytu. Zwraca również uwagę na konieczność współpracy instytucji finansowych z organami ścigania w przypadku pojawienia się incydentów bezpieczeństwa. KNF zobowiązuje banki do zachowania bezpieczeństwa w zakresie prowadzenia rachunków bankowych. Wspomniane rekomendacje określają oczekiwania organów nadzoru odnośnie praktyk stosowanych przez banki.

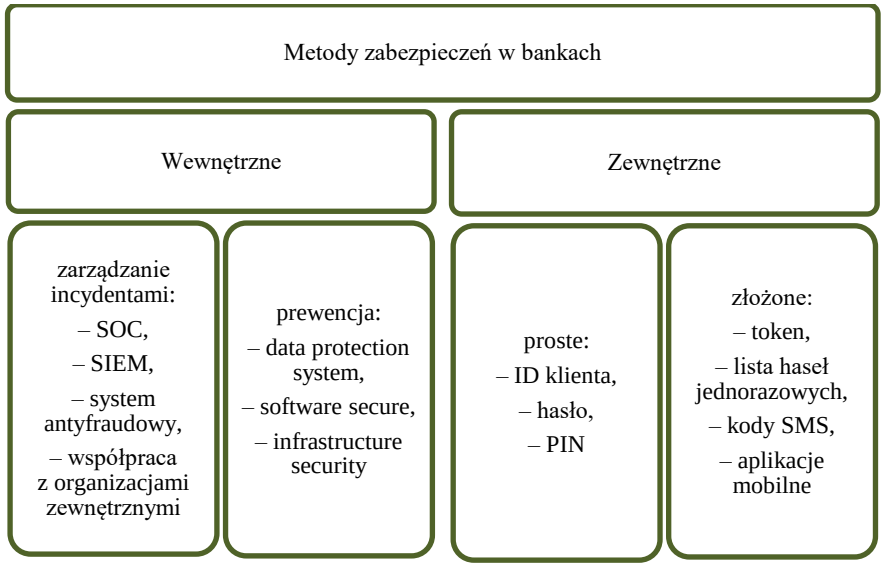
Z drugiej strony, za najistotniejsze należy uznać ustalenia zawarte w umowie o prowadzenie rachunku bankowego, ponieważ to tam znajdują się prawa i obowiązki obu stron umowy. Art. 50. ust. 1 ustawy Prawo bankowe mówi bowiem o tym, że „Posiadacz rachunku bankowego dysponuje swobodnie środkami pieniężnymi zgromadzonymi na rachunku. W umowie z bankiem mogą być zawarte postanowienia ograniczające swobodę dysponowania tymi środkami". Ustawa o usługach płatniczych również wskazuje umowę o prowadzenie rachunku bankowego jako podstawowy dokument regulujący prawa i obowiązki obu stron.

Między innymi nakładając na klienta banku obowiązek korzystania z instrumentów płatniczych (których przykładem jest karta płatnicza) zgodnie z umową ramową, odpowiedniego zabezpieczenia instrumentu płatniczego, nieudostępniania go osobom nieuprawnionym, a w przypadku utraty lub kradzieży tego instrumentu, niezwłocznego kontaktu z bankiem. Niezastosowanie się do powyższych obowiązków może skutkować, w przypadku utraty środków na rachunku, negatywnym rozpatrzeniem reklamacji oraz brakiem zwrotu pieniędzy. Dlatego też niezwykle istotny jest, w przypadku wystąpienia zagrożenia bezpieczeństwa środków (incydentu bezpieczeństwa), niezwłoczny kontakt z instytucją finansową prowadzącą rachunek. Banki każde zgłoszenie badają indywidualnie, ustalając okoliczności domniemanego przestępstwa i na podstawie przeprowadzonej analizy podejmują decyzję o zwrocie środków na rachunek lub nieuznaniu reklamacji, w przypadku braku zachowania należytej staranności zasad bezpieczeństwa ze strony posiadacza rachunku.

Bezpieczeństwo systemu bankowego jest w literaturze definiowane jako ochrona i zapobieganie atakom hakerów na prywatność, informacje oraz środki klientów banków (Li i in., 2021: 64). Bezpieczeństwo wspomnianych danych jest w głównej mierze uzależnione od systemu informatycznego oraz samych klientów. Dlatego tak ważne jest odpowiednie zabezpieczenie dokumentów elektronicznych oraz sposobu uwierzytelniania użytkowników. Każdy bank samodzielnie określa sposoby ochrony wspomnianych poufnych informacji, uwzględniając ryzyka, jakie wiążą się z ich ewentualną utratą. Można wyróżnić następujące kategorie ryzyk: finansowe (konieczność zwrotu środków utraconych przez klientów, opłaty za kary administracyjne czy – w dalszej perspektywie – zmniejszenie przychodów), czasowe (czasowa utrata dostępu do konta przez klientów, blokada środków na rachunku), reputacyjne (utrata reputacji banku w związku z wyciekiem danych klientów, podszywanie się pod korespondencję lub stronę banku), psychologiczne (awersja użytkowników do ryzyka związanego z korzystaniem z nowoczesnych technologii i usług oferowanych przez instytucje finansowe), wydajności (ataki *Distributed Denial of Service*, czyli atak na serwer z wielu urządzeń jednocześnie w celu spowodowania niedostępności usługi lub infrastruktury, malware i inne), poufności (utrata danych wrażliwych w związku z brakiem odpowiednich zabezpieczeń), prawne (reklamacje, kary administracyjne, utrata licencji).

2. METODY ZABEZPIECZEŃ STOSOWANE PRZEZ BANKI

Banki, starając się dochować należytej staranności w zakresie zapewnienia bezpieczeństwa nieustannie pracują nad rozwojem metod autoryzacji, aby były one skuteczne, przyjazne w użytku przy jednoczesnym obniżeniu kosztów eksploatacji wspomnianych zabezpieczeń.



Rysunek 1. Metody zabezpieczeń w bankach

Źródło: opracowanie własne na podstawie: Brakoniecki i in., 2015: 10.

Wśród „wewnętrznych" metod zabezpieczeń po stronie banków należy wskazać te systemowe i procesowe, np. systemy monitorujące (*Security Operation Center*, dalej: SOC), zabezpieczające i anty-fraudowe, systemy typu *Security Information and Event Management* (dalej: SIEM) oraz polityka powdrożeniowych testów produkcyjnych (Brakoniecki i in., 2015: 10). Metody zabezpieczeń wewnętrznych można podzielić na te związane z zarządzaniem incydentami naruszenia bezpieczeństwa oraz prewencyjne. Zarządzanie incydentami odnosi się do procesów i czynności takich jak SOC, SIEM, system antyfraudowy, współpraca z organizacjami zewnętrznymi, następujących po wystąpieniu zagrożenia dla bezpieczeństwa danych bądź środków konsumenta. Działania prewencyjne mają za zadanie zapobiegać występowaniu zagrożeń poprzez ich wcześniejsze zidentyfikowanie. Są to: ochrona danych (*Data Protection System*), bezpieczeństwo tworzonego oprogramowania (*software security*) oraz zapewnienie odpowiedniego poziomu zabezpieczeń infrastruktury oraz komunikacji (*infrastructure security*). Od strony infrastruktury systemowej, a także zakresu przetwarzania i analizy danych, metody zarządzania incydentami oraz prewencji często bazują na tych samych narzędziach, ponieważ są ze sobą silnie powiązane. Wykorzystywane narzędzia systemowe są tak skonstruowane, aby zapewnić nie tylko raporty

okresowe czy analizę danych historycznych, ale też w czasie rzeczywistym generować alerty (Brakoniecki i in., 2015: 24–25).

„Zewnętrzne" metody zabezpieczeń dotyczą uwierzytelniania klientów i autoryzacji transakcji w bankach. Można je podzielić na proste (identyfikator klienta, hasło, PIN) oraz złożone (tokeny, lista haseł jednorazowych, kody transakcji przesyłane przez SMSy, aplikacje mobilne). Dodatkową formę zabezpieczenia mogą stanowić obrazki bezpieczeństwa wybierane przez użytkownika przy otwieraniu konta internetowego. Najczęściej podczas logowania, na stronie internetowej banku, wyświetla się wybrany przez klienta obrazek, który stanowi dla użytkownika potwierdzenie, że znajduje się na autentycznej stronie instytucji.

Wiele zmian w zakresie metod autoryzacji wprowadziła unijna dyrektywa PSD2 (*Payment Services Directive 2*). Głównym celem jej wprowadzenia było zabezpieczenie środków finansowych przed kradzieżą, zmniejszenie odpowiedzialności za nieautoryzowane transakcje a także pełniejszy obraz finansów (Hałasik-Kozajda i Olbryś, 2021: 269). Z perspektywy klientów instytucji finansowych najbardziej odczuwalną zmianą było wprowadzenie silnego uwierzytelnienia, polegającego na podwójnej weryfikacji tożsamości konsumentów. Podwójna autoryzacja polega na wykorzystaniu co najmniej dwóch elementów z trzech kategorii: wiedza (coś, co wie wyłącznie użytkownik, np. hasło lub numer PIN), posiadanie (coś, co ma wyłącznie użytkownik, np. karta płatnicza, kod autoryzacyjny) lub cechy klienta (coś charakterystycznego wyłącznie dla użytkownika, np. wszelkie formy biometrii) (www2).

Zgodnie z powyższym zestawieniem do najpopularniejszych metod autoryzacji wykorzystywane są głównie kody SMS oraz mobilna autoryzacja. Na szczególną uwagę zasługuje autoryzacja biometryczna za pośrednictwem aplikacji mobilnej. Większość dużych banków oferuje współcześnie logowanie do aplikacji przy użyciu odcisku palca. Część instytucji wprowadziła również autoryzację przy użyciu biometrii twarzy, a nawet głosu. Biometria pozwala potwierdzić tożsamość użytkownika dzięki wykorzystaniu niepowtarzalnych cech, dlatego zdaje się być bardziej wydajna i niezawodna niż poleganie wyłącznie na czynnikach ludzkich (Morake i in., 2021: 1–10). Nie oznacza to jednak, że biometrię uznać należy za „święty Graal" autoryzacji. Jej słabe punkty zależą od wybranej metody (np. odciska palca – ryzyko fizycznego uszkodzenia, rozcięcia, biometria twarzy – utrudnienia podczas noszenia maseczki). Wśród głównych wyzwań tej metody można wskazać: wysoki koszt wdrożenia dla instytucji, brak sprzętu umożliwiającego klientowi autoryzację, niską jakość skanera, uszkodzenia mechaniczne części ciała wykorzystywanych do autoryzacji, a nawet fałszerstwo. Niestety, wraz z postępem technologicznym rośnie też zagrożenie cyberprzestępczością i choć aktualnie kradzież tożsamości biometrycznej nie jest zjawiskiem powszechnie spotykanym i kojarzy się raczej z filmami *science-fiction*, w przyszłości może się okazać równie wrażliwa jak inne aktualnie dostępne metody weryfikacji.

Tabela 2. Metody autoryzacji dostępne w przykładowych polskich bankach

Nazwa banku	Kod SMS	Token mobilny/ sprzętowy	Karta zdrapka	Serwis telefoniczny	Mobilna (w tym biometria)
Santander	TAK	NIE	NIE	NIE	TAK
Millenium	TAK	NIE	NIE	NIE	TAK
BNP Paribas	TAK	NIE	NIE	NIE	TAK
Pekao	TAK	NIE	NIE	NIE	TAK
mBank	TAK	NIE	NIE	NIE	TAK
Alior	TAK	NIE	NIE	NIE	TAK
Getin (Noble Bank)	TAK	NIE	NIE	NIE	TAK
ING	TAK	NIE	NIE	NIE	TAK
PKO BP	TAK	TAK	TAK	NIE	TAK

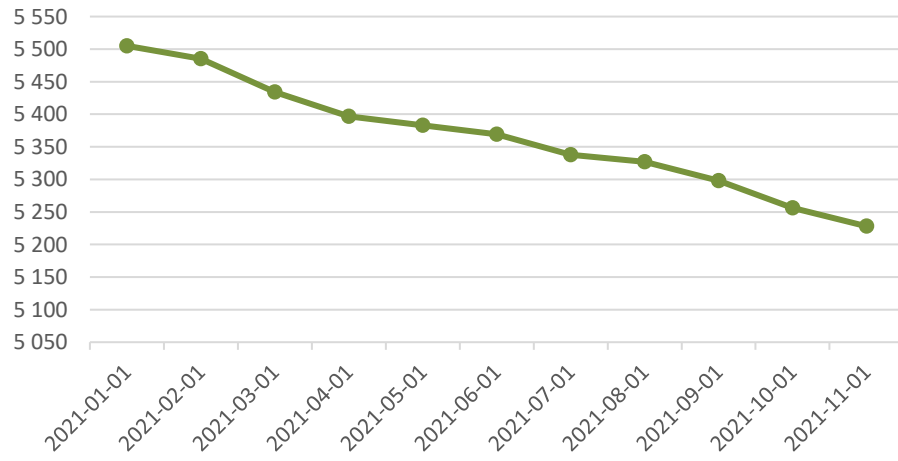
Źródło: opracowanie własne na podstawie danych dostępnych na stronach internetowych poszczególnych banków.

Podczas poszukiwania odpowiednich metod zabezpieczeń instytucje finansowe stają również przed dodatkowymi wyzwaniami: muszą one być akceptowalne pod względem kosztów, szeroko dostępne, ale też chroniące prywatność użytkowników. Na przestrzeni lat banki opracowywały różne metody autoryzacji, jednak nie zawsze były one możliwe do wdrożenia na szeroką skalę. PKO Bank Polski pracował nawet nad stworzeniem specjalnego pióra, które miało przeprowadzać autoryzację podpisu w czasie rzeczywistym (www4). Weryfikacja miała odbywać się czteroetapowo, z wykorzystaniem pióra biometrycznego, kamery, mikrofonów oraz skanera naczyń krwionośnych dłoni. Aktualnie jednak żaden z banków polskich nie korzysta z tak złożonej metody autoryzacji. Poza generowaniem wysokich kosztów w związku z przygotowaniem odpowiedniej infrastruktury technologicznej, metoda ta mogłaby budzić również pewne obawy po stronie użytkowników względem ich prywatności. Wszystkie stosowane urządzenia musiałyby być podłączone do komputera konsumenta oraz przechowywane na serwerach bankowych w celu weryfikacji. To z kolei mogłoby wraz z rozwojem cyberprzestępczości wiązać się z ryzykiem kradzieży poufnych danych. Dlatego też budowanie i utrzymywanie zaufania odnośnie bezpieczeństwa środków i informacji jest jednym z głównych wyzwań stawianych instytucjom finansowym (Hapuarachchi i Samarakoon, 2020: 1–10). Istnieją badania, które potwierdzają pozytywną zależność między zaufaniem konsumentów a ich stosunkiem wobec adaptacji nowych produktów i usług oferowanych przez bankowość elektroniczną (Al-Gharaibah, 2020: 23–39).

Warto podkreślić, że nawet najlepsze zabezpieczenia przygotowane przez bank mogą nie wystarczyć w przypadku braku rozwagi posiadacza rachunku. Częstą przyczyną utraty środków z rachunku bankowego jest korzystanie z publicznych sieci, udostępnianie danych do logowania/danych z karty płatniczej osobom trzecim czy kliknięcie w fałszywy link. Korzystanie z e-bankowości może być postrzegane jako bardziej ryzykowne, szczególnie w przypadku logowania się przez użytkowników do serwisów przy użyciu otwartych sieci. Pełne bezpieczeństwo bankowości elektronicznej uzależnione jest więc od współpracy instytucji finansowych tworzących całą infrastrukturę technologiczną i rozsądnego wykorzystania nowych technologii przez użytkowników.

3. RACHUNKI BANKOWE W POLSCE

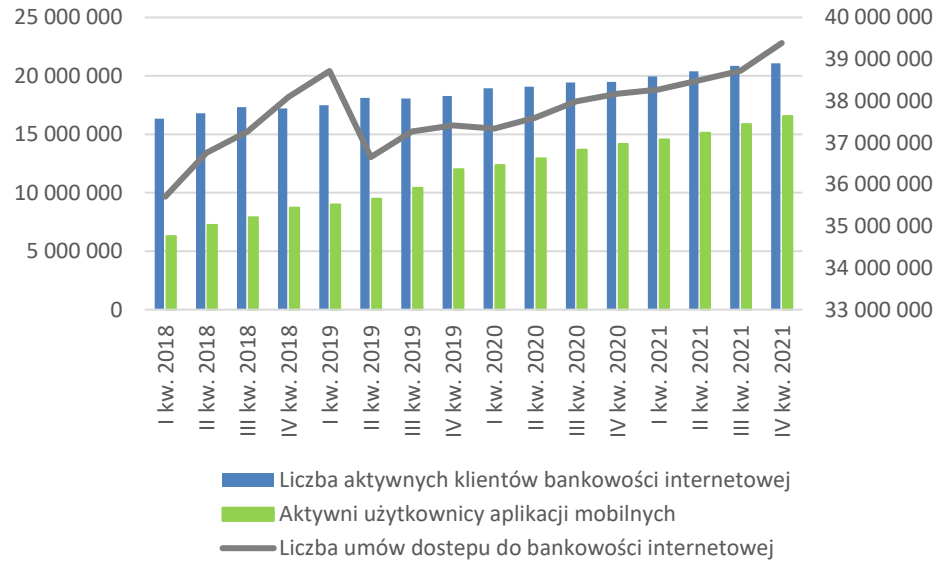
Rachunek bankowy jest narzędziem wykorzystywanym przez banki do prowadzenia rejestru należności lub powstałych zobowiązań użytkownika rachunku w stosunku do jednostki banku (Kosiński i in., 2017: 15). Bank świadczy usługi dla swojego klienta, który staje się usługobiorcą realizowanych zleceń bankowych. Klienci podejmują interakcję z instytucjami bankowymi za pośrednictwem wielu kanałów komunikacji (Tam i Oliveira, 2017: 1042–1065). Można wskazać tu choćby oddziały (których liczba drastycznie spada), bankomaty, bankowość telefoniczną, elektroniczną czy mobilną (m-banking), która nabiera coraz większego znaczenia w dokonywanej transformacji cyfrowej.



Wykres 1. Liczba oddziałów banków w okresie styczeń–listopad 2021

Źródło: opracowanie własne na podstawie bazy danych UKNF (2021).

W Polsce na koniec III kw. 2021 r. istniało blisko 38,7 mln rachunków osobistych. Jak wskazuje wykres 2, to ponad 730 tys. rachunków więcej, niż w analogicznym okresie w 2020 r. Warto zauważyć, że wspomniane dane dotyczą kont aktywnych, jednak nie ma możliwości weryfikacji regularności korzystania przez klientów z rachunków bankowych. Klienci zakładają konta bankowe z różnych powodów, wśród których poza standardową potrzebą posiadania rachunku bankowego w celu dokonywania płatności elektronicznych, można wyróżnić wnioskowanie o kredyt hipoteczny czy akcje promocyjne banków. Celem organizowania przez bank akcji promocyjnych jest zwiększenie liczby klientów aktywnie korzystających z oferowanych produktów, natomiast celem użytkowników konta jest zdobycie nagrody (wpływ określonych środków na konto, bony zakupowe, promocyjne oprocentowanie lokat czy rachunków oszczędnościowych) po spełnieniu określonych przez bank warunków. W efekcie, istnieje wiele wygaszonych i nieaktywnych rachunków powstałych w wyniku działań promocyjnych (www5). Takie sytuacje mają dość istotny wpływ na postrzegane statystyki bankowe, a jeszcze większy na bezpieczeństwo tożsamości i środków – użytkownicy często korzystają z tych samych haseł do wszystkich serwisów, a w 2018 r. 70% Polaków deklarowało brak ich zmiany w ciągu ostatnich 12 miesięcy (Związek Banków Polskich, 2018: 6).



Wykres 2. Liczba użytkowników bankowości elektronicznej

Źródło: opracowanie własne na podstawie raportów kwartalnych Netbank www3.

Liczba umów dostępu do bankowości internetowej na przestrzeni lat 2018–2021 wzrosła o 2,7 mln. W ujęciu kwartalnym wartość ta nie cechowała się tendencją wzrostową, co widoczne jest zwłaszcza w I połowie 2019 roku, gdy na przestrzeni kwartałów nastąpiła zmiana w raportowaniu tej wartości przez PKO Bank Polski (www3, Raport kwartalny Netbank Q2 2019: 6). W tym samym okresie podobnym zmianom uległa również liczba aktywnych klientów bankowości internetowej. Z kolei liczba aktywnych aplikacji mobilnych stale wzrastała. W IV kwartale 2019 roku z tej formy korzystał już niemal co piąty użytkownik. Świadczy to o coraz większym znaczeniu mobilności w bankowości elektronicznej ogółem. Smartfon staje się narzędziem pierwszego kontaktu z usługami bankowymi z uwagi na łatwy dostęp do urządzenia w każdej chwili. Wzrost zainteresowania aplikacjami mobilnymi wynika z ich nieustannego rozwoju dokonywanego przez instytucje finansowe (poszerzanie usług dostępnych w kanale mobilnym). Koniecznością staje się zatem zwrócenie szczególnej uwagi na tworzenie zabezpieczeń zwłaszcza tych kanałów dostępu.

4. INCYDENTY ZAGROŻENIA BEZPIECZEŃSTWA I ŹRÓDŁA ICH WYSTĘPOWANIA

Rozwój nowych technologii niesie za sobą zarówno wiele szans, jak i zagrożeń. Pomimo, że banki nieustannie próbują być kilka kroków przed oszustami stosując szereg działań prewencyjnych, przestępcy wyszukują dostępne luki w celu kradzieży danych osobowych lub zasobów finansowych. Na przestrzeni ostatnich lat oszuści doskonalili się nie tylko pod względem łamania zabezpieczeń systemowych, ale też kompetencji behawioralnych (miękkich), aby przy pomocy różnych technik manipulacji nakłonić potencjalną ofiarę do pożądanych działań, jednocześnie nie wzbudzając podejrzeń. Bazują w głównej mierze na trudnych emocjach, które usypiają czujność ofiar, takich jak lęk, współczucie, poczucie zagrożenia bezpieczeństwa, presja (czasu), które w połączeniu ze sobą skutkują z góry zaplanowanymi działaniami. Przestępcy identyfikują najsłabsze ogniwo w łańcuchu bezpieczeństwa, szczególnie w procesie aktywacji i odblokowania usług elektronicznych, w celu: kradzieży tożsamości, podmiany beneficjenta przelewu lub ataku socjotechnicznego na proces autoryzacji transakcji, zmiany maksymalnego limitu przelewu, zaciągnięcia zobowiązań o charakterze kredytowym. Ataki dotyczące bankowoci elektronicznej stają się coraz bardziej wyrafinowane i skomplikowane, uwzględniają specyfikę danej instytucji (Brakoniecki i in., 2015: 39).

Zestawienie w tabeli 3 stanowi pewnego rodzaju uogólnienie, ma na celu wstępne usystematyzowanie występujących zagrożeń w zależności od rodzaju serwisu, z którego korzysta użytkownik. Przedstawione zestawienie nie stanowi jednak sztywnych ram, co oznacza, że poszczególne typy oszustw mogą występować niezależnie od wybranej kategorii bankowości elektronicznej.

Tabela 3. Powszechne metody ataków z podziałem na najczęstsze miejsce występowania

Bankowość internetowa	Bankowość mobilna	Płatności z użyciem kart
Phishing danych	Utrata urządzenia mobilnego	Skimming
Pośrednictwo podmiotów trzecich	Nieuprawniona wymiana danych pomiędzy urządzeniami	Odczyt danych z karty zbliżeniowej
Złośliwe oprogramowania	Kody QR	Nieuprawnione wykorzystanie karty zbliżeniowej
Oszustwa przy zakupach przez Internet		
Przejęcie kontroli nad urządzeniem		
Oszustwa nigeryjskie/matrymonialne		

Źródło: opracowanie własne na podstawie: Krzysztoszek 2017: 5.

Phishing stanowi jedną z najbardziej popularnych metod wykorzystywanych przez cyberprzestępców. Polega na przechwyceniu danych wrażliwych (loginów, haseł, danych osobowych). Oszuści podszywając się pod instytucje, najczęściej: banki, firmy kurierskie czy serwisy transakcyjne, stosują kampanie mailingowe z prośbą o wykonanie określonych czynności (zalogowanie się do banku, dopłacenie do przesyłki/rachunku, weryfikację danych) przy użyciu „podrobionej" strony wskazanej w wiadomości mailowej. Mogą w ten sposób pozyskać od ofiary login i hasło do logowania, kody autoryzacyjne, dane z kart płatniczych. Pierwsze ataki tego typu wykryto już w 2008 roku. Na przestrzeni lat phishing ewoluował a intensywność i częstotliwość jego występowania rosła. Od 2014 roku celem ataków phishingowych były nie tylko banki, ale i większe serwisy e-commerce. Nową odmianą tego typu ataków jest *spearphishing* (włócznia) skierowany do skonkretyzowanej grupy osób lub organizacji (Brakoniecki i in., 2015: 10, 21).

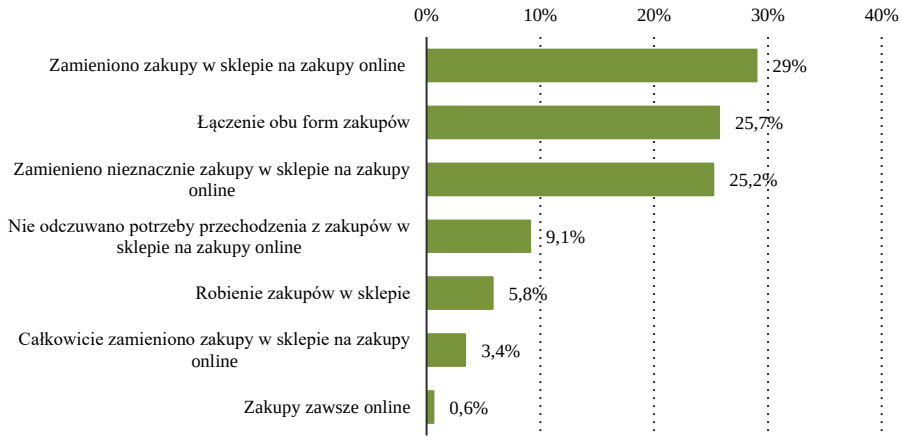
Pośrednictwo podmiotów trzecich może stanowić zagrożenie dla bezpieczeństwa danych i środków (a nawet być powodem odrzucenia reklamacji przez bank w przypadku ich utraty) ponieważ strona pośrednika nie przekierowuje użytkownika na oficjalną stronę banku, a pozostawia wszelkie dane w swoim interfejsie, wykonując operację przelewu we własnym zakresie, co może być interpretowane jako udostępnienie danych do logowania osobom trzecim (Krzysztoszek, 2017: 13).

Pierwsze ataki złośliwego oprogramowania (*malware*) w Polsce pojawiły się wraz z oprogramowaniem typu ZEUS i GOZI (tzw. koń trojański) w 2007 roku. *Malware* może szkodzić zainfekowanemu urządzeniu w mniejszym lub większym stopniu, od zwykłego spowolnienia systemu po blokadę urządzenia i kradzież poufnych informacji. Hakerzy, w celu rozprzestrzeniania złośliwego oprogramowania mogą wykorzystywać wiadomości e-mail, strony internetowe i nośniki danych. Walka z *malware* jest niewątpliwie asymetryczna. Mimo zaawansowanych

technik ochronnych oferowanych przez dostawców usług, to hakerzy, jako podmioty inicjujące, mają ułatwione zadanie ze względu na „swobodę" w wyszukiwaniu słabych punktów (Sikorski i Honing, 2012: 321–322). Podczas gdy dostawcy usług skupiają się na obronie ataków i łataniu luk w systemach, twórcy malware ulepszają swoje kody, czyniąc swoje złośliwe oprogramowania i botnety bardziej solidnymi i szkodliwymi (Rossow, 2013: 43–67). Bot jest oprogramowaniem instalowanym na urządzeniu ofiary, które dołącza do sieci podmiotów (botnet). System dowodzenia i kontroli wydaje polecenia - operacje szkodliwe – ataki typu „odmowa usługi", zbieranie danych osobowych i haseł logowania, czy wysyłanie spamu (Andriesse i Bos, 2014: 1–3).

W związku z dynamicznie rosnącą liczbą użytkowników e-bankowości, coraz częściej dochodzi do prób przejęcia kontroli nad urządzeniem konsumenta. Może się to odbywać z wykorzystaniem wyżej omawianego złośliwego oprogramowania wysłanego do potencjalnej ofiary drogą SMS lub e-mail. Haker przejmuje dane logowania do panelu bankowego oraz narzędzia autoryzacyjnego w postaci SMS (poprzez przekierowania na inny numer telefonu). Posiadając tak szeroki dostęp, oszust może nie tylko ukraść środki ulokowane na rachunku bankowym, ale też zaciągnąć dodatkowe zobowiązania.

Kolejnym zagrożeniem są oszustwa przy zakupach przez Internet. Pandemia COVID-19 w istotny sposób wpłynęła na zwiększenie wolumenu zakupów online. Te z kolei stanowią dla oszustów kolejną okazję do kradzieży, ponieważ zapewniają w dużym stopniu anonimowość.



Wykres 3. Odsetek konsumentów, którzy w związku z pandemią koronawirusa (COVID-19) w Polsce w 2021 r. zastąpili zakupy w sklepach stacjonarnych zakupami online

Źródło: Statista (2021).

Osobie niedoświadczonej w zakupach online niekiedy trudno jest odróżnić prawdziwą aukcję od tej fałszywej, szczególnie, że oszuści znają świetne sposoby na stwarzanie pozorów wiarygodności (jak na przykład fałszywe opinie od innych kupujących). Sprzedawcy często celowo ograniczają możliwość płatności wyłącznie do przelewu bankowego, podając fałszywy numer rachunku. Poszkodowany dowiaduje się o oszustwie najczęściej z kilkudniowym opóźnieniem, gdy nie otrzymuje zakupionego towaru.

Coraz bardziej popularne stają się oszustwa bazujące na ludzkich emocjach. Chociaż nie są one stosunkowo nową metoda oszustwa (od kilku lat funkcjonuje metoda „na wnuczka" czy wyłudzenie środków przez podanie kodu BLIK dla członka rodziny/przyjaciela znajdującego się w pilnej potrzebie), to oszuści w dalszym ciągu skutecznie pozyskują kolejne ofiary. W przypadku oszustw na nigeryjskiego księcia prowadzona była kampania mailingowa, w której przestępca prosił daną osobę o przelanie środków na zagraniczny numer rachunku, najczęściej z kraju afrykańskiego. W zamian za chwilową pożyczkę, taka osoba miała uzyskać w przyszłości znaczne korzyści majątkowe. Najczęściej kampanie były skierowane w osoby, które w niedawnym czasie wystawiły przedmiot na aukcji internetowej za pośrednictwem złośliwego robota (Krzysztoszek, 2017: 17). Drugi rodzaj oszustw, szczególnie bazujących na ludzkich uczuciach, to tzw. „romance fraud". Polega na stworzeniu bliskiej więzi emocjonalnej z potencjalną ofiarą, aby następnie wyłudzić od niej środki finansowe, np. na bilety lotnicze, operację członka rodziny bądź rzekome problemy finansowe (Buil-Gil i Zeng, 2021: 23).

Kolejnym zagrożeniem dla danych klientów i środków mogą okazać się po prostu w pełni aktywne aplikacje mobilne umożliwiające użytkownikom pełną obsługę swojego konta. Utrata takiego urządzenia (np. poprzez zgubienie lub kradzież) może spowodować wiele niedogodności zarówno dla posiadacza urządzenia – klienta, jak i dla banku. Przy utracie urządzenia najważniejszą kwestią jest szybkość reakcji klienta, jak również metody zabezpieczeń jakie wcześniej stosował, tj. czy urządzenie było chronione hasłem albo PINem. Istotnym aspektem są również zabezpieczenia zastosowane po stronie banku, dotyczące logowania (np. wykorzystanie do tego celu biometrii), czy też wszelkie możliwości zdalnego zablokowania aplikacji bankowej w telefonie (np. poprzez kanał zdalny z poziomu komputera/kontakt z infolinią). Niestety, niezabezpieczone w żaden sposób urządzenie daje potencjalnemu „znalazcy" pełny dostęp do skonfigurowanych płatności zbliżeniowych (poprzez NFC). Dodatkowo, proste hasło lub pin do aplikacji bankowej umożliwi takiej osobie nie tylko kradzież środków zgromadzonych na rachunku, ale też skorzystanie z innych usług bankowych nawet takich jak zaciągnięcie pożyczki gotówkowej w imieniu pierwotnego posiadacza (podobnie jak w przypadku przejęcia kontroli nad urządzeniem przez hakera).

Technologia NFC pozwala w łatwy sposób przekazywać między sobą dane w urządzeniach, jednak może zostać wykorzystana, aby w nieuprawniony sposób przejąć dane z urządzeń potencjalnych ofiar. Wykorzystywany do tego celu specjalny przyrząd może pozwolić na przechwycenie sygnału, który jest przekazywany przez moduł NFC (znajdujący się np. w telefonie). Sygnałem tym mogą stanowić dane karty podpiętej do telefonu przekazywane do terminala podczas płatności. W ten sposób przestępca może uzyskać dostęp do karty, a w dalszej kolejności wykonywać przy jej pomocy nieuprawnione transakcje.

Ataki z wykorzystaniem kodu QR mogą zostać przeprowadzone poprzez wysłanie fałszywego kodu QR SMSem, mailem, lub też mogą zostać umieszone np. na fałszywej broszurze bankowej. Przy użyciu kodu QR użytkownik ma możliwość uzyskania pewnych informacji, np. odnośnika do pobrania aplikacji bankowych. W rzeczywistości, po zeskanowaniu fałszywego kodu QR telefon zostaje zainfekowany i posłuży hakerowi do przejęcia pełnej kontroli nad urządzeniem. W konsekwencji, pozwoli to na wykonywanie wszelkich czynności na telefonie potencjalnej ofiary np. przechwycenie danych wysyłanych przez bank (haseł pierwszego logowania, kody autoryzacyjnych), a ostatecznie może to skutkować kradzieżą środków, a nawet tożsamości użytkownika telefonu.

Transakcje zbliżeniowe są bardzo prostym sposobem na dokonywanie płatności, ponieważ są praktycznie bezproblemowe w obsłudze dla klienta. Dodatkowo, nie przy każdej transakcji wymagane jest podanie kodu PIN (transakcje do kwoty 100 zł nie zawsze muszą być akceptowane przy jego użyciu). Ta niewątpliwa dogodność może sprawić, że po zagubieniu karty przestępca może w łatwy sposób ukraść z konta kilkaset złotych np. robiąc zakupy w różnych sklepach, jednak fizyczna utrata karty nie jest jedyną przyczyną utraty środków. Przestępcy mogą również wyposażyć się w przystosowany terminal, który będzie okradał ofiary, poprzez przebywanie z nimi w bliskiej odległości. Zagrożenie tego rodzaju kradzieżą jest szczególnie wysokie w zatłoczonych miejscach, gdzie przestępca w łatwy sposób może przyłożyć terminal (schowany np. w torbie) do kieszeni ofiary (ponieważ to zazwyczaj tam, w portfelu, chowamy kartę) i wykonać transakcje na ustaloną kwotę (np. 99 zł aby nie był wymagany kod PIN). Jednym z zabezpieczeń przed takimi oszustwami może być portfel ze specjalną kieszonką na kartę która zagłuszy sygnał *Radio-Frequency Identification* (w skrócie RFID, oznacza identyfikację za pomocą fal radiowych) i tym samym uniemożliwi wykonanie transakcji.

Wyżej wymienione metody oszustw to tylko niektóre z współcześnie występujących zagrożeń dla środków przechowywanych na rachunkach bankowych. Bezpieczeństwo poufnych danych użytkowników, posiadanych przez nich środków i urządzeń zależy nie tylko od zabezpieczeń przygotowywanych przez instytucje finansowe czy dostawców usług, ale i samych konsumentów. Niezwykle istotne jest korzystanie z dobrodziejstw technologicznych z rozwagą oraz bieżące

śledzenie kampanii bezpieczeństwa prowadzonych przez banki, Komisję Nadzoru Finansowego, instytucje rządowe i pozarządowe. Warto w tym miejscu przytoczyć hasło kampanii mBanku „Nie robisz tego w realu? Nie rób w sieci!", której celem było zwrócenie uwagi na ryzykowne zachowania użytkowników bankowości online oraz konsekwencje z nimi związane.

5. ANALIZA BADAŃ ANKIETOWYCH

By zidentyfikować ocenę poziomu bezpieczeństwa środków bankowych z perspektywy klientów, w okresie październik-listopad przeprowadzono ankietowe badanie online, którego kwestionariusz wypełniły 222 osoby. W związku z tym, że celem badania była ocena użytkowników usług bankowych, zdecydowano się na zredukowanie wielkości próby o rekordy zawierające odpowiedzi osób, które nie zadeklarowały posiadania rachunku (5). Ostateczna wielkość próby wyniosła 217. Próba miała charakter nielosowy, jako metodę doboru respondentów zastosowano metodę kuli śnieżnej.

Pierwsze z zadanych pytań dotyczyło odczucia co do bezpieczeństwa przechowywania środków na rachunkach bankowych. Wśród 217 respondentów 6,5% wskazało na możliwe niebezpieczeństwo, 12,5% ankietowanych nie określiło przechowywania środków bankowych ani za bezpieczne, ani za niebezpieczne, nie wyrażając wyraźnego zdania, zaś ponad 4/5 osób wyraziło swoją pewność co do zachowania bezpieczeństwa rachunków bankowych. Wskazać należy, iż liczba respondentów, która jest przekonana o bezpieczeństwie swoich środków jest porównywalna z liczbą osób, które deklarują, że ich bank prowadzi politykę bezpieczeństwa dotyczącą ochrony danych klienta (84%). W tym pytaniu znajduje się jednak 12% respondentów, którym trudno jednoznacznie określić czy polityka bezpieczeństwa jest prowadzona lub też nie oraz 4% osób, które wskazują, iż bank w ogóle nie podejmuje procedur na rzecz ochrony klienta. Sytuacja ta może mieć swoje podłoże w niewyraźnej komunikacji między bankiem a klientem i może wynikać z jego niewiedzy na temat działalności banku, gdyż zgodnie z obowiązującymi normami, każdy bank zobowiązany jest do prowadzenia takiej polityki.

Kolejne pytanie dotyczyło częstotliwości stosowanej polityki bezpieczenstwa. Docelowo pytanie skonstruowano tak, by określić częstość prowadzonych kampanii informacyjnych czy też dokonywania podwójnej weryfikacji przy zleceniach przelewów wysokokwotowych. Ponad połowie respondentów trudno było odnieść się także do samej częstotliwości prowadzonych działań na rzecz bezpieczeństwa. Można wskazać, iż problematyczną kwestią jest określenie tej częstotliwości w podanych w kweationariuszu interwałach czasowych, aniżeli braku takiej częstotliwości (wśród odpowiedzi dostępna była opcja, która równoznaczna była z niestosowaniem przez bank owej polityki). Wśród osób, które zidentyfikowały tę częstotliwość zdecydowana większość ankietowanych określiła,

że komunikaty związane z polityką bezpieczeństwa są zauważalne raz w miesiącu. 12% stwierdziło, że wiadomości nawiązujące do bezpieczeństwa widzą co tydzień, a co dziesiąty ankietowany – raz na kwartał.

Wykres 4. Częstotliwość stosowanej przez banki polityki bezpieczeństwa w opinii klientów

Źródło: opracowanie własne.

Tabela 4. Efektywność form przekazu informacji dotyczących bezpieczeństwa

Ocena	SMS-y informacyjne	Wiadomości e-mail	Rozmowa z konsultantem Contact Center	Powiadomienia push	Poczta tradycyjna	Kampanie reklamowe
5	35%	28%	13%	20%	6%	9%
4	19%	25%	14%	19%	9%	17%
3	23%	22%	27%	23%	15%	18%
2	11%	12%	11%	16%	17%	20%
1	12%	13%	35%	22%	53%	36%
Suma	100%	100%	100%	100%	100%	100%

Źródło: opracowanie własne.

Analizując ocenę formy przekazu informacji dotyczących bezpieczeństwa okazuje się, że najbardziej nieefektywną z punktu widzenia klientów metodą jest wysyłanie tradycyjnych listów informujących o niebezpieczeństwach w banko-

wości. Stwierdziło tak 53% ankietowanych i zarazem jedynie 6% tych respondentów określiło tę metodę jako przemawiającą do użytkownika. Wśród form, które uzyskały najwięcej ocen wskazujących na ich efektywność i właściwy przekaz znalazły się sms-y informacyjne oraz wiadomości e-mail, na które wskazało odpowiednio 35% i 28% ankietowanych. Negatywnie o tych metodach wypowiada się niewiele ponad jedna na dziesięć osób, co w porównaniu z innymi występującymi w zestawieniu formami stanowi niewielki odsetek.

Wśród 217 osób, jedynie 27 (12%) w odpowiedzi na pytanie dotyczące styczności z sytuacją zagrażającą bezpieczeństwu wskazała, iż takowa miała miejsce. Wśród najczęstszych przyczyn tej sytuacji wymieniano wyłudzenie danych do logowania do bankowości.

Wykres 5. Najczęstsze incydenty bezpieczeństwa wśród respondentów

Źródło: opracowanie własne.

Kolejne najczęściej występujące incydenty bezpieczeństwa opierają się na podszywaniu się pod pracownika banku, wyłudzaniu danych kart płatniczej czy przejęciu kontroli nad telefonem z dostępem do aplikacji mobilnej. Choć w badaniu występuje jedynie jedna odpowiedź dotycząca próby oszustwa na BLIK, w ostatnim czasie również była to dość powszechna metoda, która stosowana przez hakerów skutkowała utratą środków z rachunków bankowych.

Zaistniałe sytuacje wywołane incydentami bezpieczeństwa stanowiły podstawę dla podejmowania działań zarówno przez klientów jak i same banki. Reakcje z dwóch stron prezentuje zestawienie w tabeli 5.

Tabela 5. Kroki podjęte przez klienta i przez bank w sytuacji wystąpienia incydentu bezpieczeństwa

Kroki podjęte przez klienta	Liczba odpowiedzi	Kroki podjęte przez bank	Liczba odpowiedzi
Kontakt z bankiem prowadzącym rachunek, na którym wystąpił incydent bezpieczeństwa	20	Blokada narzędzia autoryzacyjnego	16
Kontakt ze wszystkimi instytucjami prowadzącymi rachunki bankowe w celu zabezpieczenia pozostałych środków	1	Blokada dostępu do kanałów zdalnych	8
Niezwłoczne zalogowanie do bankowości elektronicznej w celu zabezpieczenia środków (zmiana hasła, blokowanie dostępów przez kanały zdalne, przelanie środków na inny rachunek, blokada narzędzia autoryzacyjnego)	8	Próba anulowania przelewów niezleconych przez Klienta	5
Kontakt z policją	8	Powiadomienie organów ścigania	3
Kontakt z bliskimi	6	Reset haseł	1
Bank pierwszy podjął kontakt	1	Notatka w systemie	1
Żadne	1	Żadne	1
		Konsultant potwierdził próbę oszustwa w systemie	1

Źródło: opracowanie własne.

Wśród najczęstszych reakcji ze strony klientów wskazuje się na kontakt z bankiem – wśród 27 osób wskazujących na zetknięcie się z incydentem bezpieczeństwa kontakt ten podjęło 20 respondentów. Ośmiu ankietowanych natychmiast zalogowało się do bankowości elektronicznej, by zmienić swoje hasło i tyle samo osób podjęło kontakt z policją. Wśród 27 ankietowanych jeden respondent wskazał na zainicjowanie kontaktu w sprawie incydentu przez sam bank.

Z kolei wśród najczęściej podejmowanych kroków przez instytucje bankowe respondenci wskazują blokadę narzędzi autoryzacyjnych, blokadę dostępu do kanałów zdalnych oraz próbę anulowania przelewów niezleconych przez klienta. Wśród trzech przypadków związanych z naruszeniem bezpieczeństwa środków klienta, bank zawiadomił organy ścigania, zaś pojedyncze osoby wskazały na zaproponowany przez bank reset haseł, wykonanie notatki w systemie oraz potwierdzenia tej próby.

Tylko u czterech osób spośród 27 incydent bezpieczeństwa skutkował utratą środków pieniężnych. Wśród metod respondenci wymieniali przelanie środków na inny rachunek bankowy lub ich wypłatę w gotówce (np. poprzez kod BLIK).

Na pytanie, czy udane środki udało się odzyskać, dwie odpowiedzi wskazały, iż nie było to możliwe, jeden respondent odzyskał je dzięki współpracy banku i organów ścigania, zaś ostatnia z udzielonych przez respondentów odpowiedzi wskazuje na niepamięć co do odzyskania małej kwoty.

PODSUMOWANIE

Bazując na ustaleniach teoretycznych jak i przedstawionej analizie empirycznej można zauważyć, że instytucje bankowe są zaangażowane w tworzenie ram informujących klientów o potencjalnych niebezpieczeństwach związanych z bankowością. Są do tego zobowiązane poprzez szereg norm regulacyjnych stworzonych przez instytucje sprawujące nadzór nad sektorem bankowym. Wciąż jednak bezpieczeństwo środków klientów zależy od nich samych ze względu na coraz większe zaangażowanie cyberprzestępców w branżę usług bankowych. Stosowane zabezpieczenia nie zawsze stanowią pewne narzędzie zabezpieczające środki, stąd stosowana polityka bezpieczeństwa musi zmierzać w kierunku przekonującym klientów do podejmowania ostrożnych zachowań w sieci. Badania własne wykazały, że klienci w zdecydowanej większości bezpieczeństwo usług bankowych definiują jako właściwe, a wśród stosowanych form informujących o niebezpieczeństwie wskazują na wysoką efektywność bezpośrednich form przekazu, tj. sms-ów informacyjnych jak i wiadomości mailowych. Należy jednak zaznaczyć, że analizowana próba badawcza nie miała charakteru losowego, przez co wniosków tych nie można uogólniać na całą populację. Odnosząc się do pytania badawczego postawionego we wstępie, należy pozytywnie ocenić działania banków, które dbają o bezpieczeństwo rachunków bankowych swoich klientów poprzez: zabezpieczenia wewnętrzne infrastruktury informatycznej (SOC, SIEM, system antyfraudowy, współpracę z organizacjami zewnętrznymi, *data protection system, software secure* oraz *infrastructure secure*). Dodatkowo, banki nieustannie analizują i dostosowują swoje działania do przepisów prawnych, czego efektem były działania zabezpieczające logowanie klientów do bankowości elektronicznej (unikalne ID Klienta, obrazki logowania, hasło, PIN, logowanie za pomocą biometrii) oraz autoryzacji transakcji (token, lista haseł jednorazowych, kody SMS, aplikacje mobilne umożliwiające wykorzystywanie biometrii). Aby zwiększyć świadomość klientów, instytucje finansowe stosują również szereg kampanii informacyjnych przestrzegających przed atakami oszustów z wykorzystaniem różnych kanałów: telewizja, wiadomości SMS, wiadomości e-mail, komunikaty PUSH w aplikacji, informacje na stronach internetowych banków. Podsumowując, instytucje z odpowiednim zaangażowaniem dbają o bezpieczeństwo rachunków bankowych swoich klientów.

BIBLIOGRAFIA

Alansari, Y. i Al-Sartawi, A.M.M. (2021). IT governance and E-banking in GCC listed banks. *Procedia Computer Science*, 183. https://doi.org/10.1016/j.procs.2021.03.008.

Al-Gharaibah, O.B. (2020). Predictors of E-banking Service Adoption in Malaysia Using an Extended Technology Acceptance Model. *Int. J. Contemp. Manag. Inf. Technol*, 1(1).

Alkahtani, H., Aldhyani, T.H. i Al-Yaari, M. (2020). Adaptive anomaly detection framework model objects in cyberspace. *Applied Bionics and Biomechanics*, 1–2. https://doi.org/10.1155/2020/6660489.

Andriesse, D. i Bos, H. (2014). *An Analysis of the Zeus Peer-to-Peer Protocol*. Technical Report IR-CS-74.

Brakoniecki, M., Olczak, M. i Uryniuk, J. (2015). *Bezpieczeństwo bankowości elektronicznej. II Raport Specjalny*. https://obserwatorium.biz/wp-content/uploads/2018/11/2_PL.pdf [dostęp 15.11.2021].

Buil-Gil, D. i Zeng, Y. (2021). Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-02-2021-0042.

Freij, Å. (2020). Using technology to support financial services regulatory compliance: current applications and future prospects of regtech. *Journal of Investment Compliance*, 21(2/3). https://doi.org/10.1108/joic-10-2020-0033.

Hałasik-Kozajda, M. i Olbryś, M. (2021). Skutki implementacji dyrektywy o usługach płatniczych (PSD2). *Bank i Kredyt*, 52(3).

Hapuarachchi, C. i Samarakoon, A. (2020). Drivers Affecting Online Banking Usage of Private Commercial Banks in Sri Lanka. *Asian Journal of Economics, Business and Accounting*, 20(1).

Jibril, A.B., Kwarteng, M., Chovancova i M., Denanyoh, R. (2020), *Customers' Perception of Cybersecurity Threats Toward e-Banking Adoption and Retention: A Conceptual Study*,15th International Conference on Cyber Warfare and Security, 275.

Kosiński, B., Nowak, A., Karkowska, R. i Winkler-Drews, T. (2017). *Podstawy Współczesnej Bankowości*. Warszawa: Polskie Wydawnictwo Ekonomiczne.

Krzysztoszek, M. (2017). *Bankowość elektroniczna w teorii i praktyce*. Warszawa: Komisja Nadzoru Finansowego.

Le Nguyen, C. (2018). Preventing the use of financial institutions for money laundering and the implications for financial privacy. *Journal of Money Laundering Control*, 21(1).

Lenka, S.K. i Barik, R. (2018). Has expansion of mobile phone and internet use spurred financial inclusion in the SAARC countries? *Financial Innovation*, 4(5). https://doi.org/10.1186/s40854-018-0089-x.

Li, F., Lu, H., Hou, M., Cui i K., Darbandi, M. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*, 64. https://doi.org/10.1016/j.techsoc.2020.101487.

Lisowska, A. i Waściński, T. (2021). Bezpieczeństwo bankowości internetowej i mobilnej na rynku finansowym. *Systemy Logistyczne Wojsk*, 54. https://doi.org/10.37055/slw/140380.

Liyanaarachchi, G., Deshpande, S. i Weaven, S. (2021). Online banking and privacy: redesigning sales strategy through social exchange. *International Journal of Bank Marketing*, 39(6). https://doi.org/10.1108/IJBM-05-2020-0278.

Melnychenko, S., Volosovych, S. i Baraniuk, Y. (2020). Dominant ideas of financial technologies in digital banking. *Baltic Journal of Economic Studies*, 6(1). https://doi.org/10.30525/2256-0742/2020-6-1-92-99.

Morake, A., Khoza, L.T. i Bokaba T. (2021). Biometric technology in banking institutions: 'The customers' perspectives'. *SA Journal of Information Management*, 23(1). https://doi.org/10.4102/sajim.v23i1.1407.

Mościeanu, D., Roxana, N., Faccia, D., Cavaliere, L.P.L. i Bhatia, S. (2020). Digital technologies' implementation within financial and banking system during socio distancing restrictions – back to the future. *International Journal of Advanced Research in Engineering and Technology*, 11(6).
Nosowski, A. (2005). Geneza bankowości elektronicznej. W: A. Gospodarowicz, red., *Bankowość elektroniczna*. Warszawa: PWE.
Omariba, Z.B., Masese, N.B. i Wanyembi, G. (2012). Security and privacy of electronic banking. *International Journal of Computer Science Issues (IJCSI)*, 9(4).
Rossow, C. (2013). *Using Malware Analysis to Evaluate Botnet Resilience.* PhD Thesis, Amsterdam: Vrije Universiteit.
Sikorski, M. i Honing, A. (2012). *Practical malware analysis. The hands-on guide to dissecting malicious software*. San Francisco: No starch press.
Tam, C. i Oliveira, T. (2017). Literature review of mobile banking and individual performance. *International Journal of Bank Marketing*, 35(7). https://doi.org/10.1108/IJBM-09-2015-0143.
(www1) https://cert.pl/raporty-roczne/ [dostęp 3.11.2022].
(www2) https://prnews.pl/wp-content/uploads/2020/12/polska_bankowosc_w_liczbach_IIIq2020.pdf [dostęp 25.11.2021].
[www3] https://www.zbp.pl/raporty-i-publikacje/raporty-cykliczne/raport-netbank [dostęp 13.01.2022].
[www4] https://rf.gov.pl/2020/07/30/rachunek-podstawowy-darmowe-rozwiazanie [dostęp 03.12.2021].
Związek Banków Polskich (2018). *Cyberbezpieczny portfel*. Warszawa.

Akty prawne

Dyrektywa 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE. L. z 2016 r. nr 119, str. 1 z późn. zm.).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego.
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (wersja przekształcona) (Dz.U. UE. L. z 2016 r. nr 26, str. 19 z późn. zm.).
Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf [dostęp 11.11.2021].
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
Uchwała Komisji Nadzoru Bankowego z dnia 11 grudnia 2002 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki.
Uchwała Nr 7/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz.Urz. KNF z 2013 r. poz. 5).
Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. 2021, poz. 1907 z późn. zm.).
Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. 2021, poz. 2439 z późn. zm.).

Zakończenie recenzji/ End of review: 20.11.2022
Przyjęto/Accepted: 02.12.2022
Opublikowano/Published: 22.12.2022