ŚRODOWISKO BEZPIECZEŃSTWA KLIENTÓW BANKOWOŚCI ELEKTRONICZNEJ

SYGN. WIB PAB 19/2021

Raport opracowany na zlecenie Programu Analityczno-Badawczego
Fundacji Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY

Gdynia, wrzesień, 2021

PROGRAM ANALITYCZNO BADAWCZY

O Raporcie

Raport **Środowisko bezpieczeństwa klientów bankowości elektronicznej** został opracowany na zlecenie Programu Analityczno-Badawczego Fundacji Warszawski Instytut Bankowości

Autorzy:

Raport przygotowany przez zespół w składzie:

Jerzy Kosiński
– profesor nadzwyczajny Akademii Marynarki Wojennej w Gdyni, dyrektor Morskiego Centrum Cyberbezpieczeństwa AMW. Do 2018 pełnił służbę w Policji zajmując się cyberprzestępczością, dowodami cyfrowymi, białym wywiadem internetowym i naruszeniami własności intelektualnej w internecie (odchodził na emeryturę jako prorektor ds.studiów Wyższej Szkoły Policji w Szczytnie). Organizator cyklicznych konferencji międzynarodowych „Techniczne aspekty przestępczości teleinformatycznej" (20 edycji), które w 2018 roku zmieniły nazwę na „Przestępczość teleinformatyczna XXI" (2 edycje). Autor wielu publikacji i wystąpień na konferencjach z zakresu swojej specjalności naukowej. Biegły sądowy z zakresu przestępczości komputerowej i kart płatniczych z listy Sądu Okręgowego w Olsztynie.

dr hab. Grzegorz Krasnodębski
– profesor nadzwyczajny Akademii Marynarki Wojennej w Gdyni, z-ca dyrektora Morskiego Centrum Cyberbezpieczeństwa AMW. Absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej. W latach 1994-2004 pracował w Zespole Informatyki Marynarki Wojennej jako programista, projektant oraz analityk przy tworzeniu systemów informatycznych dla Marynarki Wojennej RP.
Od 2004 roku zajmował stanowiska wykładowcy, adiunkta oraz kierownika w Zakładzie Zarządzania Kryzysowego na Wydziale Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej. W latach 2015–2019 pełnił funkcję Prodziekana ds. Nauki na Wydziale Dowodzenia i Operacji Morskich.
Specjalizuje się w zagadnieniach związanych z zarządzaniem kryzysowym, ochroną infrastruktury krytycznej, wykorzystaniem systemów informatycznych w bezpieczeństwie oraz cyberbezpieczeństwem.

Paweł Ciszek
– doktor w dyscyplinie nauk o bezpieczeństwie, starszy specjalista Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni, Członek Morskiego Centrum Cyberbezpieczeństwa, wcześniej oficer bezpieczeństwa informacji Proservice Finteco. Do 2019 roku pełnił służbę w Policji zajmując się technologiami informacyjnymi, bezpieczeństwem informacji, zwalczaniem przestępczości teleinformatycznej. Współorganizator konferencji „Techniczne aspekty przestępczości teleinformatycznej" i „Przestępczość teleinformatyczna XXI". Były biegły sądowy z zakresu przestępczości komputerowej i kart płatniczych z listy Sądu Okręgowego w Olsztynie.

Paweł Wawrzyniak
– Senior Technology Risk Manager w międzynarodowej instytucji finansowej, członek Morskiego Centrum Cyberbezpieczeństwa. Zawodowo związany z branżą IT od 2000 roku. Szczególnie interesuje się problematyką szeroko rozumianego cyberbezpieczeństwa i cyberodporności w kontekście transformacji cyfrowej banków. Prelegent wielu konferencji branżowych. Łączy kompetencje humanistyczne i techniczne, wykorzystując je w różnych obszarach IT. Od 2019 roku wykładowca akademicki.

PROGRAM ANALITYCZNO BADAWCZY

O Programie

Program Analityczno-Badawczy przy Fundacji WIB powstał w 2019 roku jako odpowiedź na potrzeby sektora bankowego w zakresie analizy zjawisk, tworzenia opracowań i porządkowania wiedzy w obszarach cyberbezpieczeństwa i nowych technologii, a także szeroko rozumianego otoczenia sektora bankowego, kształtującego warunki działania banków w Polsce. Prace analityczno-badawcze w ramach programu realizowane są pod kątem możliwości praktycznego wykorzystania ich wyników w celu rozwoju sektora bankowego, podnoszenia poziomu bezpieczeństwa usług oraz kreowania wartości dla klientów bankowości. PAB WIB kładzie duży nacisk na rozwój współpracy ze środowiskami akademickimi i eksperckimi, poszukując synergii w zakresie zainteresowań badawczych autorów oraz potrzeb rozwojowych sektora bankowego.

W ramach programu realizowane są analizy i badania w następujących obszarach:

- **Nowe technologie i cyberbezpieczeństwo**
- **Zdolność banków do finansowania gospodarki**
- **Bankowość spółdzielcza**
- **Rynek nieruchomości**
- **Zielony ład i finansowanie energetyki odnawialnej**
- **Finansowanie projektów innowacyjnych**

Więcej na temat działalności programu na stronie www.pab.wib.org.pl

Kontakt:

dr Andrzej Banasiak
Koordynator Programu
m: 696 405 104
e: abanasiak@wib.org.pl

Jacek Gieorgica
m: 603 626 254
e: jgieorgica@wib.org.pl

Warszawski Instytut Bankowości
00-394 Warszawa, ul. Solec 38, lok 104
t: (22) 182 31 70
e: pab@wib.org.pl

Agnieszka Nierodka
m: 607 484 391
e: anierodka@wib.org.pl

dr Tomasz Pawlonka
m: 505 917 778
e: tpawlonka@wib.org.pl

Spis treści

Streszczenie kierownicze

Celem głównym niniejszego raportu była analiza środowiska bezpieczeństwa klienta bankowości elektronicznej, a w szczególności:

– charakterystyka istniejących rozwiązań dla klienta bankowości elektronicznej;

– charakterystyka klienta bankowości elektronicznej;

– identyfikacja zagrożeń dla klienta bankowości elektronicznej;

– określenie kierunków rozwoju usług dla klienta bankowości elektronicznej;

– wskazanie możliwych działań wzmacniających świadomość zagrożeń dla klienta bankowości elektronicznej.

Do osiągnięcia celów miały służyć sformułowane problemy badawcze dotyczące 3 obszarów i zawarte w następujących 5 pytaniach:

I. Część diagnostyczna – strona bankowa:

1. Jakie rozwiązania techniczne i proceduralne są stosowane w bankowości elektronicznej?

2. Jakie są zdiagnozowane zagrożenia dla obecnego klienta bankowości elektronicznej?

II. Część diagnostyczna – klient bankowości:

3. Jaka jest dojrzałość technologiczna klientów bankowości elektronicznej?

4. Jaka jest świadomość zagrożeń dla klientów bankowości elektronicznej?

III. Część prognostyczna:

5. Jakie są kierunki rozwoju usług bankowych dla klienta bankowości elektronicznej?

W badaniu wykorzystano wiele metod badawczych, wśród których należy zwrócić uwagę na:

– metodę badania dokumentów – szeroka analiza dostępnego piśmiennictwa oraz zasobów Internetu stanowiła podstawę do przygotowania sondażu diagnostycznego;

– metodę sondażu diagnostycznego – w zakresie badania dotyczącego klienta bankowości elektronicznej. Przebadano 153 osoby. Arkusz kalkulacyjny z wynikami badania stanowi załącznik do raportu;

– metodę analizy indywidualnych przypadków – wykorzystaną głównie jako analiza przestępstw na szkodę klienta bankowości elektronicznej, będących podstawą pogłębionych wywiadów eksperckich;

– wywiad ekspercki z przedstawicielami rynku, sektora bankowego oraz osobami zaangażowanymi w rozwój rynku. Do badania nominowano 18 ekspertów z sektorów bankowego i IT, którzy specjalizują się w tematyce cyberbezpieczeństwa (w szczególności bankowości elektronicznej) oraz biegłych sądowych, spośród których 13 poświęciło swój czas na wspólną z zespołem analizę wyników badania dokumentów i sondażu diagnostycznego. Lista ekspertów, wraz z zapisami wywiadów lub ich transkrypcją, stanowią załącznik do raportu.

Część diagnostyczna badania potwierdziła, że bankowość elektroniczna jest otwarta na innowacje, co pociąga za sobą projektowanie i dostarczanie nowych produktów i usług. Możliwości technologiczne stają się głównym wyróżnikiem dla banków, jeśli chodzi o poprawę satysfakcji klientów. Konsekwencją szybkiego włączania nowych technologii i zaspokajania potrzeb klientów jest ogromne wyzwanie w obszarach architektury rozwiązań teleinformatycznych i cyberbezpieczeństwa.

Fundamentalną kwestią w zapewnieniu bezpieczeństwa bankowości elektronicznej jest przestrzeganie przyjętych standardów bezpieczeństwa. Głównym zagrożeniem bankowości elektronicznej zdiagnozowanym w badaniu jest socjotechnika. Warto w tym kontekście zwrócić większą uwagę na uwierzytelnianie z wykorzystaniem tokenów wspierających standard U2F, aplikacji uwierzytelniających, ale także, po

stronie banków, na monitoring behawioralny zachowania klienta.

Z badania klientów bankowości elektronicznej i wywiadów eksperckich wynika, że dojrzałość bankowości elektronicznej – w powszechnym odbiorze – jest wysoka. Dojrzałość użytkowników (klientów), rozumiana jako świadomość zagrożeń, deklaratywnie jest również wysoka, niestety realna odporność na nie już taka nie jest. Oznacza to, że banki muszą upewnić się, że nie tylko przekazują stosowną informację o zagrożeniach i właściwej reakcji na nie swoim klientom, lecz także powinny zweryfikować, czy informacja taka zostanie zapamiętana. Warto również zwrócić uwagę, że deklaratywnie klienci preferują bezpieczeństwo kosztem łatwości użytkowania, co kontrastuje z opiniami ekspertów.

Należy przyjąć, że na bezpieczeństwo klienta bankowości elektronicznej wpływają przede wszystkim: ewolucyjne zmiany technologiczne, większa transparentność, większa łatwość użytkowania (ergonomia), jak najmniej elementów wymagających uczenia się od klienta-użytkownika i odpowiednia komunikacja dotycząca zasadności oraz celowości wprowadzania zmian.

Sugerowany kierunek rozwoju, który wychodziłby naprzeciw postulatom klientocentryczności i omnikanałowości, wiąże się z powstaniem zintegrowanych platform typu „elektroniczne okienko bankowe". Powinno ono pokrywać w kanałach elektronicznej komunikacji ofertę banków w sposób całościowy. Co jednak kluczowe, musi pozwalać na taki poziom silnego uwierzytelniania i autoryzacji, który nie pozwoli na późniejsze podważenie faktu dokonania jakiejś operacji.

Zarówno klienci, jak i eksperci wskazywali, że właściwym kierunkiem podnoszenia bezpieczeństwa bankowości elektronicznej jest szersze wykorzystanie biometrii. Znacznie mniej akceptacji, głównie z uwagi na wnoszenie nowych zagrożeń, znajduje stosowanie sztucznej inteligencji.

Z badania wynika również, że kultura bankowości elektronicznej nie powinna być budowana przez każdy bank osobno, aby klienci nie zaczęli się gubić w rozmaitości pojęć, zasad i standardów. Wydaje się, że rolę lidera mógłby pełnić tutaj Związek Banków Polskich – ma to być bowiem kultura bankowości elektronicznej, a nie kultura bankowości elektronicznej określonego banku.

Wstęp

Rewolucja Informacyjna, której obecnie jesteśmy świadkami, rozpoczęła się w roku 1946, kiedy na uniwersytecie stanowym w Pensylwanii zbudowano pierwszą na świecie maszynę liczącą – ENIAC[1]. Ta zajmująca 170 m^2 powierzchni i ważąca 30 ton maszyna zdeterminowała kierunek rozwoju społeczeństw, prowadząc je systematycznie do zmian, określanych obecnie mianem Rewolucji Informacyjnej. Krokiem milowym owej rewolucji było wprowadzenie w latach 80. ubiegłego wieku przez firmę IBM pierwszego modelu komputera osobistego. Innym wydarzeniem, które odegrało poważną rolę w procesie światowej informatyzacji, było także powołanie do życia w 1957 r. przez Departament Obrony Stanów Zjednoczonych projektu ARPA[2]. Ta początkowo wojskowa, a następnie także akademicka, sieć ARPA (ARPAnet) służąca pierwotnie do wymiany poglądów pomiędzy ośrodkami akademickimi, stała się podwaliną pod największą światową sieć komputerową – Internet. W 1971 r. Ray Tomlinson opracował program do obsługi poczty elektronicznej, w 1985 r. zarejestrowano *symbolics.com* – pierwszą domenę internetową, zaś Tim Berners Lee stworzył technologię WWW (*ang. World Wide Web*) w roku 1989. W ten sposób powstał Internet ogólnie dostępny i wszechstronny, które to cechy zadecydowały o wykorzystaniu go w każdej niemal dziedzinie życia codziennego – prywatnego, zawodowego i publicznego.

Można przedstawić także inne ujęcie, a mianowicie nieznanego w historii ludzkości rozwoju zarówno technologii, jak i jej poziomu dostępności. Na początku lat 90. XX w. dostęp do Internetu posiadało około 3 miliony osób, z czego 73% pochodziło z USA, zaś 15% z Europy Zachodniej. Na przełomie wieków szacowano, że liczba użytkowników Internetu wzrosła do prawie 369 milionów osób, w 2010 r., po upływie kolejnej dekady, szacowano, że na świecie są prawie dwa miliardy użytkowników Internetu, pięć miliardów telefonów komórkowych, 255 milionów stron internetowych, zaś dziennie wysyła się ponad 294 milionów wiadomości e-mail oraz 5 miliardów SMS-ów. W roku 2012 szacowano, że spośród 7 mld mieszkańców Ziemi aż 2,4 miliarda to użytkownicy Internetu, z czego 2,2 miliarda posiadało konto poczty elektronicznej i łącznie wysyłało dziennie 144 miliardy e-maili.

Obecnie[3] na 7,8 miliarda populacji ludzkości jako internautów klasyfikuje się 5,2 miliarda ludzi, przy czym ponad 53% tej liczby przypada na Azję, dziennie wysyłanych jest 377 miliardów wiadomości e-mail, a łączna liczba telefonów komórkowych to 4,28 miliarda; dodatkowo szacuje się, że do 2025 roku ilość danych generowanych każdego dnia w Internecie osiągnie 463 eksabajtów (EB).

Prawie 1 milion dolarów na minutę wydaje się dzisiaj na zakupy w Internecie, a do roku 2030 planuje się, że 90% ludności w wieku powyżej sześciu lat będzie dostępnych online.

Rozwój cywilizacyjny doprowadził nas do punktu, gdy posiadanie dostępu do Internetu jest czymś tak powszechnym, że jego brak w domu dziwi bardziej niż brak bieżącej wody.

Internet stał się trwałym elementem naszego życia, a znaczny stopień „usieciowienia" współczesnego środowiska sprawił, że pojawiły się nowe, dotychczas niespotykane zagrożenia.

Odnalezienie się w tym dynamicznym i coraz bardziej skomplikowanym środowisku jest wyzwaniem dla każdego z nas, przy czym wyzwanie to jest o wiele większe wobec organizacji zaufania publicznego, którymi są banki.

Biorąc pod uwagę skalę zagrożenia – co 39 sekund w Internecie pojawia się nowy atak, codziennie tworzone jest ponad 1,3 mln fragmentów malware, którego jedynym celem jest kradzież danych i – w efekcie środków finansowych – rzeczą podstawowej wagi jest diagnoza środowiska, w jakim przyszło funkcjonować klientowi bankowości, który był, jest i będzie zasadniczym ogniwem bezpieczeństwa w bankowości, jaką znamy i tej, jaka nadejdzie wraz z nieuchronnym rozwojem technologicznym.

[1] Electronic Numerical Integrator And Computer.
[2] Advanced Research Project Agency.
[3] Stan na 31.03.2021 – za Internet Big Picture – https://www.internetworldstats.com/stats.htm

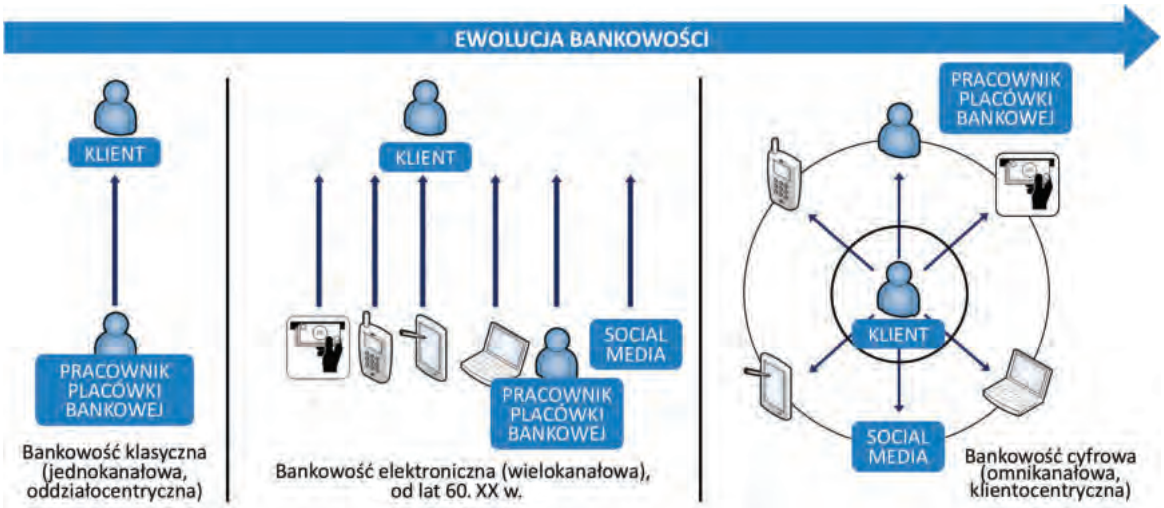
W dalszej części raportu przedstawiono wyniki:

- analizy artykułów naukowych i literatury specjalistycznej dotyczącej omawianego środowiska bezpieczeństwa klientów bankowości elektronicznej,
- badań terenowych/ankietowych klientów bankowości elektronicznej przeprowadzonych w celu określenia ich poziomu świadomości i umiejętności korzystania z bankowości elektronicznej,
- wywiadów eksperckich, do których zaproszono ekspertów z sektorów bankowego i IT, specjalizujących się w tematyce cyberbezpieczeństwa (w szczególności bankowości elektronicznej), a także biegłych sądowych.

Zaprezentowane treści są także wynikiem przeglądu raportów, wytycznych i opracowań branżowych.

Charakterystyka nowoczesnych rozwiązań dla klienta bankowości elektronicznej

Bankowość można poddać klasyfikacji ze względu na organizację dostępnych kanałów komunikacji z klientem, czyli kanałów dystrybucji, za pośrednictwem których świadczone są usługi bankowe. Ujęcie to doskonale ukazuje ewolucję bankowości, pozwala skupić się na jej technologicznym wymiarze, a także wskazuje związek między konkretnym kanałem komunikacyjnym (kanałem dystrybucji usług), a określonym rodzajem przestępczości. Schemat 1 przedstawia kierunek ewolucji od bankowości klasycznej (jednokanałowej, oddziałocentrycznej), przez bankowość elektroniczną (wielokanałową), po bankowość cyfrową (omnikanałową, klientocentryczną).



Schemat 1. Kierunek ewolucji od bankowości klasycznej (jednokanałowej, oddziałocentrycznej), przez bankowość elektroniczną (wielokanałową), po bankowość cyfrową (omnikanałową, klientocentryczną). Ukazano podstawowe kanały komunikacji między klientem a bankiem.[4]

1.1. Bankowość klasyczna, czyli bankowość jednokanałowa, oddziałocentryczna

Do lat 50. XX w. bankowość stawiała wyłącznie na bezpośredni kontakt z klientem i wymagała istnienia rozległej sieci placówek. Ten tradycyjny model bankowości funkcjonuje do dziś, nazywany jest obecnie *bankowością klasyczną*, a ponieważ placówki bankowe są tutaj jedynym kanałem komunikacji z klientami, spotyka się także takie określenia, jak *bankowość oddziałocentryczna* lub *bankowość jednokanałowa*[5].

W kontekście zagrożeń bezpieczeństwa bankowości klasycznej należy mieć świadomość, że napady lub włamania (kolokwialnie nazywane „skokami") są dużo bardziej prawdopodobne w przypadku terenowych placówek bankowych niż dobrze zabezpieczonych central i skarbców – przy czym funkcjonuje tutaj rozróżnienie: napady realizowane są przez uzbrojonych przestępców w godzinach pracy banku, a do włamań dochodzi poza godzinami obsługi klientów[6]. Osobną kategorią przestępczości związanej z bankowością klasyczną są napady na konwoje wartości pieniężnych.

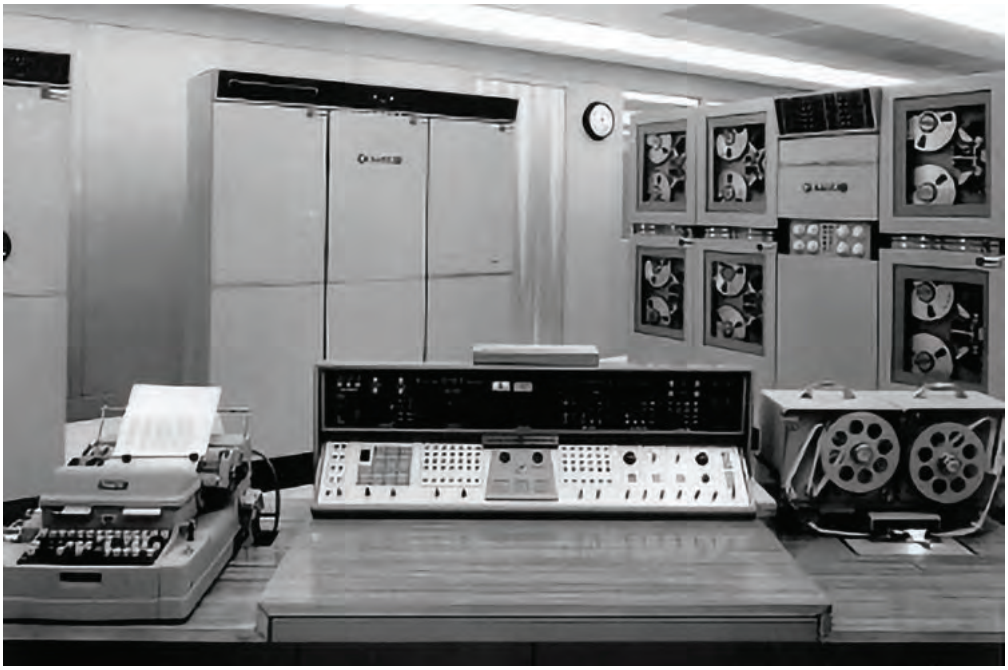
1.2. Bankowość elektroniczna, wielokanałowa

W latach 50. XX w. rozpoczęła się komputeryzacja bankowości. W 1954 roku do Bank of America dostarczono pierwszy komputer do użytku biznesowego – Remington Rand UNIVAC-1. Dane były wprowadzane do tego komputera za pomocą taśm magnetycznych, które przetwarzały się z prędkością 12 000 cyfr lub liter na sekundę. Cztery lata wcześniej Bank of America we współpracy ze Stanford Research Institute opracował pierwszy na świecie komputer do przetwarzania czeków. We wrześniu 1955 r., zaledwie rok po wprowadzeniu Remington Rand UNIVAC-1, Bank of America zaprezentował urządzenie o nazwie ERMA

[4] Na podst.: M. Rehfisch, Omnichannel Banking: *A Prerequisite for a Seamless Customer Journey*, https://www.knowis.com/blog/omnichannel-banking-a-prerequisite-for-a-seamless-customer-journey, stan z dn. 29 czerwca 2021.

[5] P. Wawrzyniak, *Ewolucja problematyki przestępczości bankowej z uwzględnieniem ważniejszych zagrożeń, [w:] „Przegląd prac konkursowych. Edycja VII (2016/2017)", pod red. E. Dąbrowskiej, Agencja Bezpieczeństwa Wewnętrznego. Centralny Ośrodek Szkolenia i Edukacji im. gen. dyw. Stefana Roweckiego „Grota", Emów, 2019.*

[6] Por.: R. Patterson, *Kompendium terminów z zakresu bankowości po polsku i angielsku, Ministerstwo Finansów, Warszawa 2015, s. 285-286.*



Fotografia 1. Konsola operatorska komputera ERMA[7]

(ang. *Electronic Recording Method of Accounting* – elektroniczna metoda zapisu księgowania). Komputer ten przetwarzał czeki i automatycznie zarządzał kontem[8] – patrz fotografia 1.

Mimo tej zmiany technologicznej nadal wyłącznym kanałem komunikacji z klientami pozostawała sieć placówek bankowych. Początkowo komputeryzacja zachodziła bowiem na zapleczach banków.

Z punktu widzenia obsługi klientów *bankowość elektroniczna* (ang. *electronic banking* lub *e-banking*) jest jednoznaczna z określeniem „zdalna bankowość", a więc oznacza korzystanie z usług bez kontaktu klientów z pracownikami banków, jedynie za pomocą łączy telekomunikacyjnych oraz urządzeń elektronicznych. Tak więc zasadniczą ideą bankowości elektronicznej jest przede wszystkim elektroniczna obsługa klientów poprzez umożliwienie włączenia się ich jako użytkowników do informatycznego systemu bankowego. W rezultacie to właśnie klient, a nie pracownik banku jest inicjatorem operacji z dala od fizycznej siedziby banku[9]. Umożliwia to istnienie wielu, równolegle dostępnych, elektronicznych kanałów komunikacji (dystrybucji), które pozwalają na świadczenie usług w sposób bezkontaktowy. Nie oznacza to jednak zaprzestania świadczenia usług bankowych w modelu klasycznym – bezpośredni kontakt w placówce banku wciąż pozostaje jedną z dostępnych metod komunikacji klienta z bankiem (dystrybucji usług bankowych), chociaż bankowość elektroniczna jest z natury rzeczy wielokanałowa, a więc oferuje alternatywne kanały komunikacji. Jednocześnie *bankowość elektroniczna* pozwala na dostęp zarówno do tradycyjnych usług, które świadczone są w wielu kanałach, jak i do całkiem nowych usług, które są następstwem wykorzystania przez bank nowoczesnych technologii.

Rozwój bankowości elektronicznej na świecie nastąpił w drugiej połowie XX wieku, w USA. Można wyróżnić jego cztery etapy:

- lata 60. – pojawienie się pierwszych bankomatów, które umożliwiły dostęp do rachunków klientów, a więc *bankowość terminalow*a.
- lata 70. – dostęp do rachunków za pośrednictwem telefonu, czyli *bankowość telefoniczna*.
- lata 80. – wykorzystanie do obsługi rachunków komputerów osobistych, a więc *bankowość komputerowo-modemowa* w odmianie domowej (ang. *home banking*) i skierowanej dla przedsiębiorców (ang. *corporate banking*).

[7] Na podst.: *ERMA and MICR, the Origin of Electronic Banking*, https://www.smecc.org/sri_erma_history.htm, stan z dn. 26 czerwca 2021.

[8] *Bank of America revolutionizes banking industry*, https://about.bankofamerica.com/en-us/our-story/bank-of-america-revolutionizes-industry.html#fbid=j4W3HuwWHH5, stan z dn. 29 czerwca 2021.

[9] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia*, Temida 2, Białystok 2011.

Fotografia 2. Pierwszy udostępniony publicznie w 1967 r. przez Barclays Bank bankomat wymagał wykorzystania specjalnych czeków, impregnowanych promieniotwórczym izotopem węgla-14, zanim klienci mogli podać swój unikalny PIN i dokonać wypłaty.[10]

– lata 90. – świadczenie usług przez Internet, a więc *bankowość internetowa*.

Za początki *bankowości elektronicznej*, a więc *wielokanałowej*, umownie przyjąć można 27 czerwca 1967 r. – wówczas Barclays Bank udostępnił publicznie pierwszy bankomat[11] – patrz fotografia 2. Tak powstał więc pierwszy, równoległy kanał dystrybucji usług.

Od tego momentu rozwój bankowości jest ściśle połączony z rozwojem nowoczesnych technologii. Fakt ten jest nie bez znaczenia, jeżeli chodzi o ewolucję przestępczości bankowej, która obecnie wymierzona jest przede wszystkim w stronę klientów.

1.3. Bankowość cyfrowa, czyli bankowość klientocentryczna, omnikanałowa

O ile za początek rozwoju bankowości internetowej (jedna z odmian bankowości elektronicznej, wielokanałowej) przyjmuje się lata 90. XX w., co wiąże się z faktem coraz większej popularyzacji Internetu i początkami handlu elektronicznego w tamtym czasie, to za umowną datę rozpoczęcia transformacji cyfrowej banków można przyjąć – symbolicznie – pojawienie się na rynku smartfonów z ekranem dotykowym (iPhone) za sprawą firmy Apple[12].

Polskie banki rozpoczęły transformację cyfrową kilka lat temu i z reguły posiadają w tym zakresie własną strategię. *Transformację cyfrową* można zdefiniować jako działania polegające na zmianie modelu biznesowego banku poprzez dostosowanie aktualnych, a także powołanie nowych procesów, narzędzi i rozwiązań (zarówno w ramach oferowanych produktów i usług bankowych – *transformacja zewnętrzna*, ale i ich obsługi oraz rozwoju kanałów dystrybucji – *transformacja wewnętrzna*), opartych na nowoczesnych technologiach, w celu sprostania ewoluującym potrzebom klientów. Początkowo procesy związane z transformacją cyfrową traktowane były jak projekty adaptacyjne do zmian rynkowych i nikt nie rozpatrywał ich w kategoriach strategicznych dla banków, nie spodziewano się bowiem, że rozwój nowych technologii będzie pozwalał na tak daleko idące zmiany w obsłudze klienta bankowego. Podstawowymi założeniami bankowości cyfrowej stały się *omnikanałowość* i *klientocentryczność*.

Omnikanałowość oznacza możliwość zmiany kanału dystrybucji w ramach jednego procesu zakupowego,

[10] Na podst.: From the archives: the ATM is 50, https://home.barclays/news/2017/06/from-the-archives-the-atm-is-50/, stan z dn. 26 czerwca 2021.

[11] B. Batiz-Lazo, R. J. K. Reid, *Evidence from the Patent Record on the Development of Cash Dispensing Technology*, https://mpra.ub.uni-muenchen.de/9461/1/MPRA_paper_9461.pdf, stan z dn. 29 listopada 2020, s.3.

[12] P. Druszcz, *Digitalizacja produktów bankowych jako cel strategiczny uczestników polskiego sektora bankowego, „Ruch Prawniczy, Ekonomiczny i Socjologiczny", Rok LXXIX, 1/2017, s. 242.*

np. klient realizuje pierwszą część kupna kredytu przez Internet (złożenie wniosku), a następnie może kontynuować realizację w innym kanale – bankowości mobilnej, telefonicznej lub w oddziale. Omnikanałowość różni się od wielokanałowości tym, że ta druga daje możliwość wykonania usługi w wielu kanałach, przy czym realizacja następuje od początku do końca w tym samym kanale. Istotą omnikanałowości nie jest więc równoległe, niezależne funkcjonowanie różnych kanałów komunikacji z bankiem, ale takie ich sprzężenie, by się wzajemnie przenikały i uzupełniały. Dzięki temu klient ma uzyskać swobodę wyboru i gwarancję jednakowego standardu obsługi oraz tej samej ceny produktu w każdym z dostępnych kanałów[13].

Z kolei *klientocentryczność* (koncentracja na kliencie) polega przede wszystkim na skupieniu się na doświadczeniach klienta połączonych z dogłębnym zbadaniem aktualnej roli oddziałów banków, co oznacza w istocie konieczność odejścia od tradycyjnej roli oddziału jako głównego kanału sprzedaży (bankowość klasyczna) na rzecz miejsca, w którym klient zasięgnie wysokiej jakości porady od prawdziwego eksperta. W związku z tym, jeszcze przez wiele lat oddziały bankowe nie znikną w bankowości cyfrowej całkowicie, chociaż należy spodziewać się, że ich liczba znacząco zmaleje. Istotne jest to, że rola oddziałów banku w kontakcie z klientem ulega zmianie.

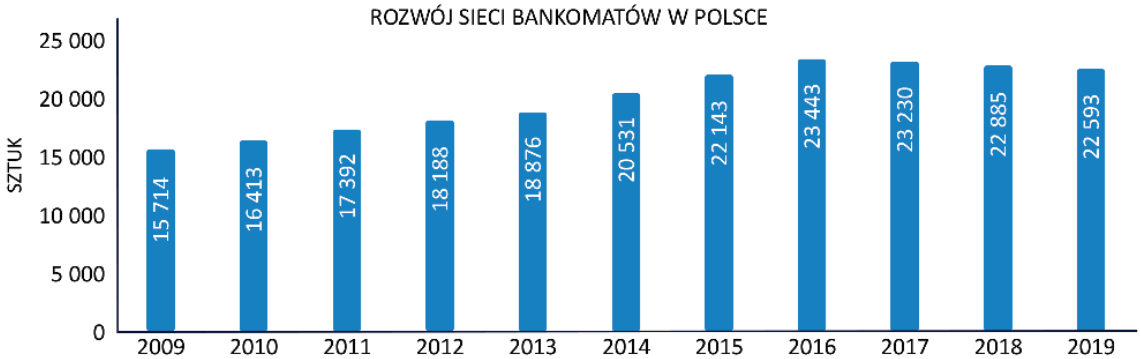
Bankowość cyfrowa musi być otwarta na innowacje, co ma objawiać się przez integrację marketingu i IT. Innowacje są tutaj podstawą projektowania i dostarczania produktów i usług. Rynek zmienia się szybko, więc konkurencyjność wymaga wysoce efektywnego połączenia pomiędzy nowymi technologiami (odpowiedzialność działu IT) a jednostkami biznesowymi banku. Zdolność do szybkiego włączania nowych technologii i zaspokajania potrzeb klientów stanowi ogromne wyzwanie w obszarach architektury rozwiązań teleinformatycznych i cyberbezpieczeństwa, a także współpracy między działami IT i biznesem. Odpowiedzią ma być tutaj *zwinność* (ang. *agile*) *technologiczno-organizacyjna*. Elastyczne platformy IT mają bowiem zasadnicze znaczenie dla digitalizacji modeli operacyjnych banków. Możliwości technologiczne stają się głównym wyróżnikiem dla banków, jeśli chodzi o poprawę satysfakcji klientów, która ostatecznie ma decydujące znaczenie dla konkurencyjności rynkowej. W tym kontekście szczególnego znaczenia nabierają także kwestie zarządzania ryzykiem technologicznym.

1.4. Sprzęt

W tym podrozdziale omówiony został wykorzystywany współcześnie sprzęt, taki jak: bankomaty (ang. *Automated Teller Machine*, ATM), terminale płatnicze (ang. *Point of Sale*, POS), karty płatnicze i urządzenia służące do obrotu walutami wirtualnymi (tzw. *bitomaty* – nazwa pochodzi od ang. *bitcoin*, czyli najpopularniejszej kryptowaluty i *bankomatu*). Scharakteryzowane zostały również najpowszechniejsze urządzenia klienta bankowości elektronicznej, takie jak komputery, laptopy, tablety, smartfony, smartwatche (i inne urządzenia typu „smart"), sprzętowe portfele kryptowalutowe itp.

1.4.1. Bankomaty

Rozwój bankomatów ewoluował od prostych urządzeń służących wyłącznie do wypłaty gotówki (ang. *cash dispenser*) do wieloczynnościowych bankomatów typu ATM (ang. *Automated Teller Machine*), które oprócz wypłaty gotówki umożliwiają dostęp do salda



Wykres 1. Rozwój sieci bankomatów w Polsce (liczebność w sztukach) w okresie od 2009 r. do trzeciego kwartału 2019 r. (K3-2019)

[13] Z. Jagiełło, *Bankowość detaliczna w obecnych warunkach rynkowych. Kierunki rozwoju, [w:] Wyzwania bankowości detalicznej, pod red. Z. Jagiełło, Instytut Badań nad Gospodarką Rynkową – Gdańska Akademia Bankowa, Gdańsk 2015, s. 10.*

[14] Na podst.: *Raport o sytuacji ekonomicznej banków. Banki 2019, Nr 10/2020, Warszawski Instytut Bankowości, Warszawa 2020, s. 91.*

rachunku, dokonywanie przelewów, udostępniają informacje i ogłoszenia banku, a nawet posiadają funkcję depozytową, czyli mogą przyjmować gotówkę w depozyt[15] (funkcja tzw. wpłatomatu). Pierwszy bankomat w Polsce został zainstalowany przez Bank Pekao S.A. w 1990 r., a więc po 23 latach od pojawienia się podobnego urządzenia w Wielkiej Brytanii. Wykres 1 przedstawia liczebność sieci bankomatów w Polsce od 2009 r. do trzeciego kwartału 2019 r. (K3-2019).

Bankomaty wyposażone są m.in. w czytnik kart, pozwalający na odczyt danych z paska magnetycznego lub mikroprocesora karty płatniczej. Większość z nich zezwala także na dokonywanie operacji za pośrednictwem systemu płatności mobilnych BLIK. Wykorzystanie bankomatów do realizacji transakcji często bywa nazywane bankowością terminalową.

1.4.2. Terminale płatnicze

Terminale płatnicze, terminale POS (ang. *Point of Sale Terminal, POS Terminal* – tł. dosłowne: terminal punktu sprzedażowego) to elektroniczne urządzenia, które instalowane są w punktach handlowo-usługowych i pozwalają na komunikację klientów z bankiem za pośrednictwem centrum autoryzacyjnego w celu uiszczenia opłaty za zakupiony towar lub usługę. Terminal POS wyposażony jest w czytnik kart, pozwalający na odczyt danych z paska magnetycznego lub mikroprocesora karty płatniczej. Możliwa jest także realizacja transakcji z wykorzystaniem systemu płatności mobilnych BLIK. Typowy zestaw terminala POS został przedstawiony na fotografii 3.[16]

Terminale płatnicze mogą pracować na standardowych łączach telekomunikacyjnych i wymagać stałego zasilania – wówczas nazywane są terminalami stacjonarnymi. Można je spotkać np. na sklepowych stanowiskach kasowych. Z kolei terminale mobilne to takie, które wyposażone są w akumulator i mogą korzystać z sieci GSM lub Wi-Fi, dzięki czemu są w stanie pracować w praktycznie dowolnym miejscu, o ile posiadają dostęp do sieci. Tego typu rozwiązania są popularne np. w restauracjach czy firmach kurierskich.

Fotografia 3. Typowy zestaw terminala POS, który można spotkać w punktach handlowo-usługowych, np. w restauracjach[16]

[15] P. Niczyporuk, A. Talecka, *Bankowość. Podstawowe zagadnienia, Temida 2, Białystok 2011.*

[16] Na podst.: *How To Test Point Of Sale (POS) System – Restaurant POS Testing Example*, https://www.softwaretestinghelp.com/how-to-test-point-of-sale-pos-system/, stan z dn. 29 czerwca 2021.

Podstawowym przeznaczeniem terminali płatniczych jest autoryzacja płatności, tzn. weryfikacja karty płatniczej i jej właściciela, przed rozliczeniem transakcji.

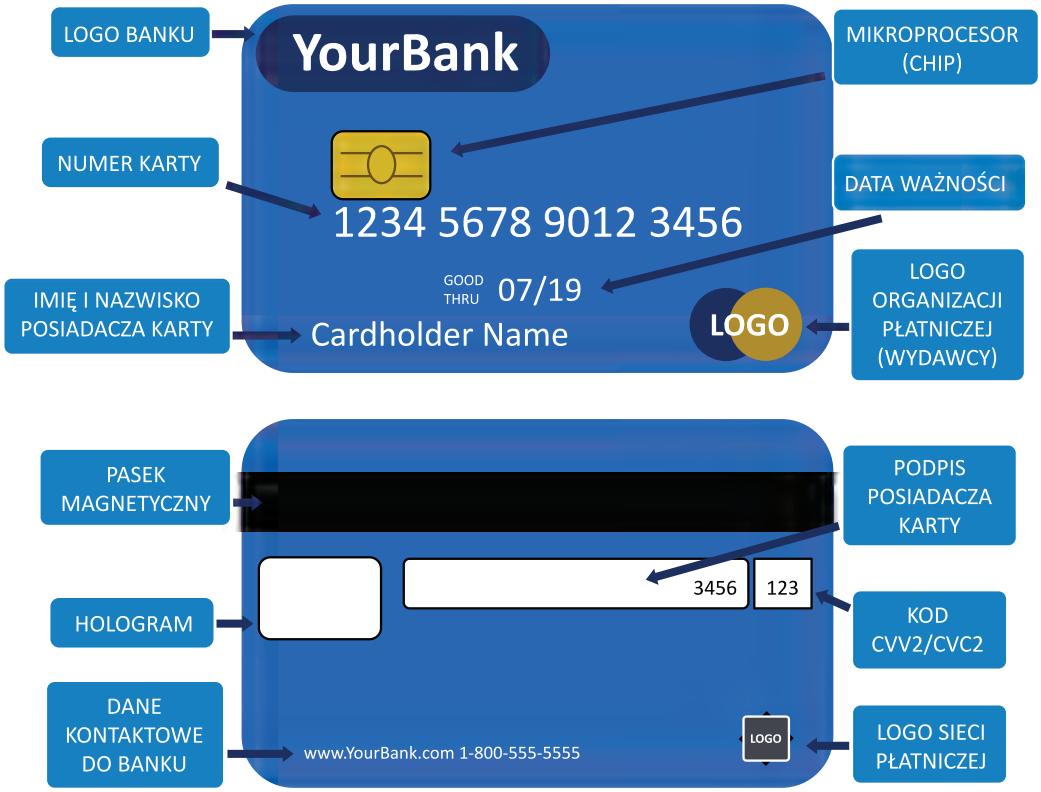
1.4.3. Karty płatnicze

Zgodnie z art. 2 pkt. 15a ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych karta płatnicza: „uprawnia do wypłaty gotówki lub umożliwia złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego" oraz jest „akceptowaną przez akceptanta w celu otrzymania przez niego należnych mu środków"[17].

Karty płatnicze mogą być wydawane przez banki lub inne organizacje – najbardziej znane to: Visa i Mastercard. Poglądowa karta płatnicza wraz z zaznaczeniem podstawowych jej elementów została przedstawiona na rycinie 1.

Karty płatnicze są instrumentami płatniczymi, które stanowią wygodną alternatywę dla płatności gotówkowych. Można używać ich do przeprowadzania transakcji związanych z zakupem towarów lub usług. Podczas zatwierdzania transakcji w terminalu POS należy zwykle podać unikalny numer PIN. Obecnie większość kart płatniczych pozwala także na transakcje zbliżeniowe. Karta może być także użyta do wypłaty środków z bankomatu. Ponadto stanowią one wygodny środek płatniczy, który jest szeroko stosowany w handlu elektronicznym w przypadku tzw. transakcji bezgotówkowych typu card not present, czyli podczas transakcji zakupu towarów i usług przez Internet (wówczas musimy podać unikalny kod CVV2/CVC2 – ang. Card Verification Value/Card Validation Code 2, czyli numer weryfikacyjny karty lub kod walidacyjny karty (w zależności od wydawcy).

Najpopularniejsze typy kart płatniczych to: karty kredytowe, karty debetowe, karty obciążeniowe, karty przedpłacone (prepaid) i karty wirtualne (nie są wydawane w fizycznej postaci, chociaż posiadają swój unikalny numer i kod CVV2/CVC2, dzięki czemu można używać ich do realizacji transakcji bezgotówkowych typu card not present).



Rycina 1. Poglądowa karta płatnicza i jej podstawowe elementy[18]

[17] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2011 nr 199 poz. 1175.

[18] Na podst.: *How To Test Point Of Sale (POS) System – Restaurant POS Testing Example*, https://www.softwaretestinghelp.com/how-to-test-point-of-sale-pos-system/, stan z dn. 29 czerwca 2021.

Fotografia 4. Przykładowy bitomat (zdj. Patrycja Malik)[19]

1.4.4. Bitomaty

Bitomaty (nazwa pochodzi od ang. *Bitcoin*, czyli najpopularniejszej kryptowaluty i *bankomatu*) to stosunkowo nowe urządzenia, które służą do obrotu kryptowalutami – możliwa jest zarówno sprzedaż (zamiana na gotówkę), jak i kupno kryptowalut za gotówkę. Bitomaty łączą więc funkcje bankomatów i wpłatomatów w odniesieniu do kryptowalut. Przykładowy bitomat przedstawiono na fotografii 4.

Obecnie na świecie zainstalowanych jest ponad 22 000 bitomatów (najwięcej w USA), w tym ponad 100 w Polsce. Jednocześnie na świecie działa 43 producentów tego typu urządzeń (np. Genesis Coin, General Bytes, BitAccess) i ponad 600 operatorów (np. Bitcoin Depot, CoinFlip, CoinCloud, Shitcoins Club)[20].

1.4.5. Smartfony

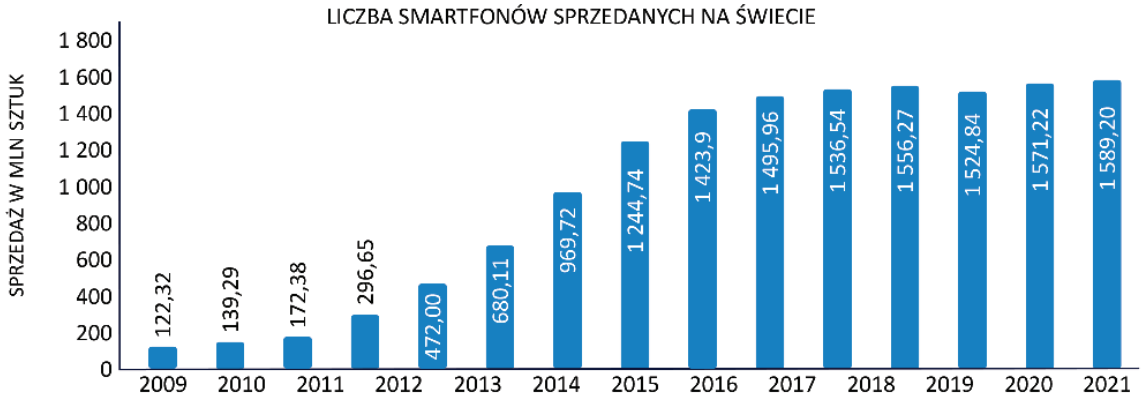
Od premiery pierwszego urządzenia typu smartfon (z ekranem dotykowym) liczba urządzeń mobilnych otwierających całkiem nowe możliwości przed bankowością zaczęła gwałtownie wzrastać – patrz wykres 2. Pojawił się też nowy kanał komunikacji z bankiem, najbardziej istotny z punktu widzenia transformacji cyfrowej banków – *bankowość mobilna*.

Smartfony to multimedialne urządzenia przenośne, które łączą w sobie funkcjonalność telefonu komórkowego i przenośnego komputera, dzięki czemu stały się wyjątkowo atrakcyjne dla bankowości – patrz fotografia 5.

Możliwość instalowania różnego rodzaju aplikacji oznacza, że ich funkcjonalność może być rozszerzana, włączając m.in. możliwość wykorzystania smartfonów do realizacji operacji bankowych, w tym zbliżeniowych płatności bezgotówkowych. Dzięki odpowiedniemu oprogramowaniu, smartfony mogą pełnić rolę prostych, mobilnych terminali POS, które są w stanie obsługiwać płatności za pomocą kart.

[19] Na podst.: *M1 i Galeria Łódzka. Pierwsze w Łodzi bitomaty do wymiany kryptowalut, https://lodz.wyborcza.pl/lodz/7,35136,23111070,w-lodzi-powstal-pierwszy-bitcoinmat-stanal-w-galerii-lodzkiej.html?disableRedirects=true, stan z dn. 29 czerwca 2021.*

[20] Na podst.: *Bitcoin ATM Map, https://coinatmradar.com/, stan z dn. 29 czerwca 2021.*



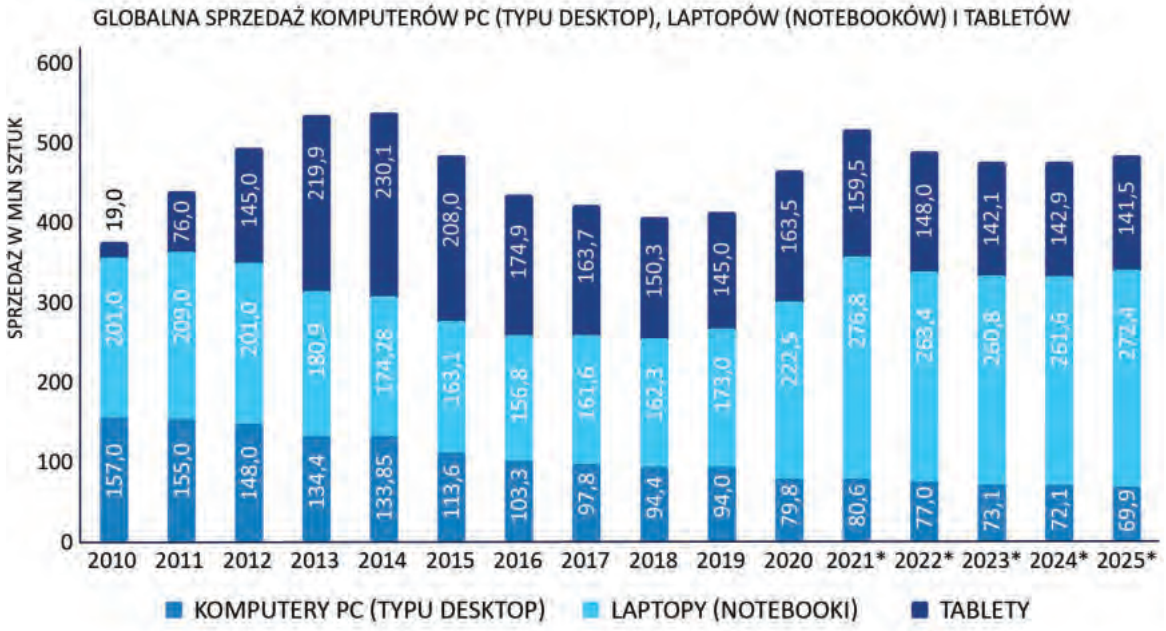
Wykres 2. Liczba smartfonów sprzedanych na świecie od 2007 r. do 2021 r. (oszacowanie). Wyraźny wzrost miał wpływ na popularyzację bankowości mobilnej[22]

Fotografia 5. Smartfony wpłynęły na rozwój bankowości mobilnej[22]

1.4.6. Komputery, laptopy, tablety

Komputery (typu desktop) i laptopy (notebooki) to urządzenia najczęściej używane do bankowości elektronicznej w odmianie internetowej, kiedy klient kontaktuje się z bankiem za pośrednictwem aplikacji webowej dostępnej w przeglądarce internetowej. W odróżnieniu od komputerów typu desktop, laptopy charakteryzują się wysoką mobilnością, dlatego stają się coraz bardziej popularne. Rozwiązaniem pośrednim wydają się być tablety, które mogą w dużym stopniu udostępniać podobny komfort użycia i funkcjonalność, jak laptopy, o ile zostaną wyposażone w zewnętrzną klawiaturę. Wydaje się jednak, że rynek tabletów po chwilowym wzroście sprzedaży w latach 2010-2015 obecnie już się ustabilizował. Notoryczny spadek sprzedaży notują natomiast komputery PC. Prawidłowości te przedstawiono na wykresie 3.

[21] Op. własne na podst.: *Number of smartphones sold to end users worldwide from 2007 to 2021 (in million units)*, https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/, stan z dn. 5 stycznia 2021.
[22] Na podst.: *Smartphone as a mobile POS (mPOS), https://medium.com/zoidcoin-network/smartphone-as-a-mobile-pos-mpos-55e-6acb6cc4b, stan z dn. 29 czerwca 2021.*



Wykres 3. Globalna sprzedaż komputerów PC, laptopów (notebooków) i tabletów w latach 2010 do 2025 (okres od 2021* do 2025* stanowi oszacowanie)[23]

Istotne jest tutaj także kryterium systemu operacyjnego, co przekłada się na dostępność określonych aplikacji dla bankowości elektronicznej. Odpowiednio możemy przyjąć, że następujące systemy operacyjne dla poszczególnych urządzeń determinują w dużym stopniu sposób, w jaki użytkownik korzysta z bankowości elektronicznej:[23]

- Komputery PC (typu desktop), laptopy (notebooki) – systemy operacyjne: Microsoft Windows, GNU/Linux, Apple MacOS. Dostęp przez przeglądarkę internetową do aplikacji webowej systemu bankowości elektronicznej.

- Tablety – systemy operacyjne: Microsoft Windows, Apple iOS, Apple iPadOS, Google Android. W przypadku MS Windows dostęp przez przeglądarkę internetową do aplikacji webowej systemu bankowości elektronicznej. Dla systemów operacyjnych Apple iOS, Apple iPadOS, Google Android możliwy jest zarówno dostęp przez przeglądarkę internetową do aplikacji webowej systemu bankowości elektronicznej, jak i wykorzystanie dedykowanej aplikacji dla bankowości mobilnej, instalowanej na urządzeniu.

Przywołane systemy operacyjne dla poszczególnych typów urządzeń reprezentują rzeczywisty rynek. W niniejszym opracowaniu nie są brane pod uwagę niszowe lub eksperymentalne rozwiązania.

1.4.7. Urządzenia typu *smart*

Chociaż technologie mobilne – utożsamiane ze smartfonami i działającymi na nich aplikacjami bankowymi – tworzą dziś najbardziej oczywisty kanał komunikacji z bankiem, to ogromny potencjał tkwi także w tzw. „urządzeniach ubieralnych" (ang. *wearables*) czy też urządzeniach typu *smart* (pol. mądry). Dzięki nim można nie tylko ułatwić kontakt klienta z bankiem, ale także mierzyć za pomocą wbudowanych sensorów szereg parametrów związanych z codzienną aktywnością użytkowników (począwszy od lokalizacji geograficznej przez wykonywane czynności po kondycję fizyczną i psychiczną, a nawet stan zdrowia), co pozwala poznać ich wzorce zachowań w określonych miejscach i czasie. Rycina 2 przedstawia najpopularniejsze rodzaje urządzeń ubieralnych.

Spośród przykładowych urządzeń ubieralnych lub typu *smart* wskazanych na rycinie 2, najbardziej rozsądnym obecnie wyborem w przypadku realizowania transakcji bankowych wydają się: zegarek (ang. smartwatch), opaska lub bransoletka (ang. *smartband* lub *smart bracelet*). Warto jednak zauważyć, że praktycznie dowolne urządzenie typu smart, które zostanie wyposażone w system operacyjny pozwalający na instalację dedykowanych aplikacji może zostać użyte do realizacji transakcji – np. zbliżeniowych płatności bezgotówkowych.

Tego typu urządzenia (obok smartfonów) wytyczają nowe kierunki rozwoju bankowości elektronicznej w odmianie mobilnej sprzyjając transformacji cyfrowej. Ich

[23] Na podst.: *Notebook, desktop PC, and tablet shipments worldwide 2010-2025 (in million units)*, https://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/, stan z dn. 30 czerwca 2021.

Rycina 2. Przykładowe urządzenia ubieralne (ang. wearables) typu smart, które pozwalają na gromadzenie szerokiego zakresu danych na temat ich użytkowników[24]

wykorzystanie wiąże się z problematyką profilowania klientów i obszarem zastosowania technologii Big Data, służącej do przetwarzania wielkich zbiorów danych. Dzięki nim banki są w stanie nie tylko spełniać postulat klientocentryczności, lepiej dostosowując ofertę do potrzeb klientów, lecz także wkraczają w całkiem nowy wymiar związany z zarządzaniem ryzykiem.

1.4.8. Sprzętowe portfele kryptowalutowe

Sprzętowe portfele (ang. *hardware wallets*) kryptowalutowe to urządzenia, które pozwalają przechowywać w bezpieczny sposób klucze prywatne użytkownika, wykorzystywane przez niego do obrotu kryptowalutami. Tego typu sprzętowe rozwiązania mają istotną przewagę nad programowymi portfelami (ang. *software wallets*) kryptowalutowymi, które działają w sieci, ponieważ klucze prywatne są przechowywane poza dyskiem twardym urządzenia wykorzystywanego do realizacji transakcji z użyciem kryptowalut i znajdują się w chronionej przestrzeni mikrokontrolera, są zaszyfrowane i nie mogą być wytransferowane poza urządzenie w postaci niezaszyfrowanej. Dzięki temu sprzętowe portfele kryptowalutowe oferują wyższy poziom bezpieczeństwa od portfeli programowych. Są m.in. odporne na ataki hakerskie i działanie złośliwego oprogramowania, które wykrada klucze z portfeli programowych. Ceny tych urządzeń mieszczą się obecnie w przedziale od kilkudziesięciu do ok. 600 PLN. Fotografia 6 przedstawia dwa przykładowe sprzętowe portfele kryptowalutowe.

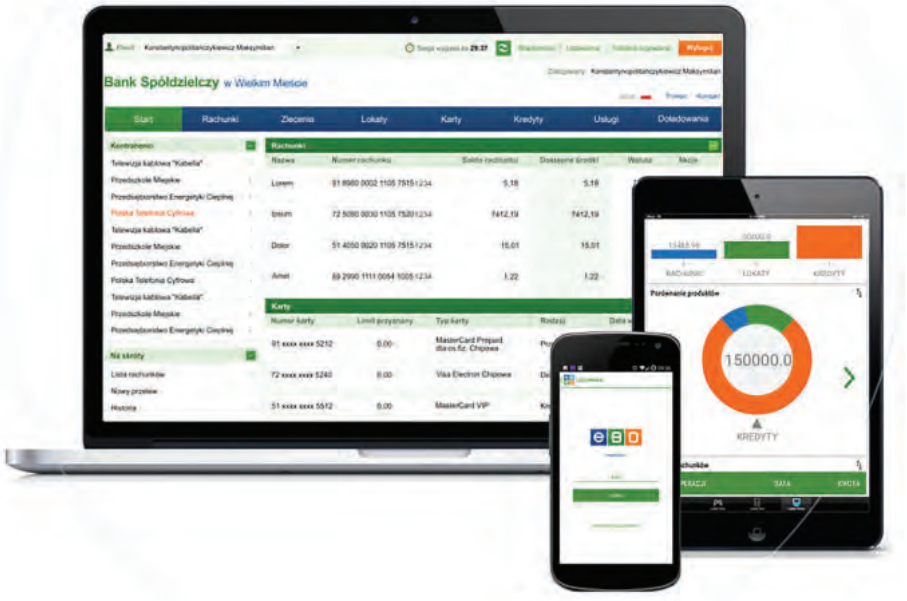
Rynek kryptowalut rozwija się dynamicznie, o czym świadczy także coraz szersza gama rozwiązań dla ich użytkowników. Należy jednak pamiętać, że banki podchodzą do nich wciąż z dużą rezerwą.

1.5. Oprogramowanie

W obszarze oprogramowania dla bankowości elektronicznej należy wymienić przede wszystkim aplikacje webowe, które dostępne są dla klientów przez przeglądarkę internetową. Pozwalają one na dostęp do systemu bankowości elektronicznej z dowolnego urządzenia, na którym może być uruchomiona przeglądarka internetowa spełniająca wymagania aplikacji. Ten kanał komunikacji wywodzi się jeszcze z lat 90., w których pojawiła się bankowość internetowa i jest do dziś powszechnie stosowany na komputerach PC (typu

[24] M. Mishra, *Rise of Wearables and future of Wearable technology*, https://medium.com/@manasim.letsnurture/rise-of-wearables-and-future-of-wearable-technology-1a4e38a2fbb6, stan z dn. 6 stycznia 2021.

Fotografia 6. Przykładowe sprzętowe portfele kryptowalutowe: po lewej – Ledger Nano X; po prawej – tani (cena 19,95 EUR) sprzętowy portfel kryptowalutowy oferowany przez BlochsTech w postaci karty płatniczej, który cechuje się łatwością użycia. Na uwagę zwraca hasło: „I am my own bank!" (pol. „Jestem swoim własnym bankiem!")[25]



Fotografia 7. Przykładowa aplikacja webowa bankowości internetowej i mobilnej Banku Spółdzielczego w Namysłowie uruchomiona na laptopie, tablecie i smartfonie[26]

desktop) oraz laptopach (notebookach), ale może być także wykorzystywany na tabletach i smartfonach.

Obecnie zakres funkcjonalności typowych aplikacji webowych dla bankowości internetowej i aplikacji mobilnych instalowanych na smartfonach oraz tabletach powoli ulega ujednoliceniu, co przekłada się na podniesienie komfortu użytkowników. Przykładowa aplikacja webowa bankowości internetowej i mobilnej została przedstawiona na fotografii 7.

Aplikacja bankowości internetowej i mobilnej pozwala zwykle wykonać wszystkie podstawowe operacje online w obszarach takich jak:

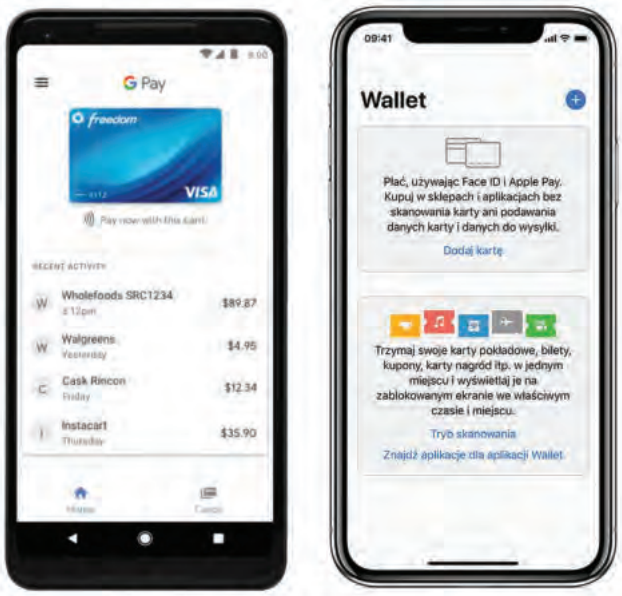
[25] Hardware wallet, https://en.bitcoin.it/wiki/Hardware_wallet, stan z dn. 3 lipca 2021.

[26] *Bankowość internetowa, https://bsnamyslow.com.pl/klienci-indywidualni/bankowo%C5%9B%C4%87-internetowa, stan z dn. 3 lipca 2021.*

- obsługa kont, rachunków, przelewów, kart debetowych i kredytowych oraz lokat;
- dostęp do informacji na temat pożyczek i kredytów oraz możliwość zaciągnięcia nowych pożyczek;
- zarządzanie funkcjami związanymi z bezpieczeństwem (np. ustalenie reguł uwierzytelniania wieloskładnikowego i autoryzacji; możliwość ustawienia zaufanej przeglądarki);
- zarządzanie limitami przelewów dla aplikacji webowej i mobilnej (zainstalowanej np. na smartfonie);
- składanie wniosków (np. o konto osobiste, walutowe lub oszczędnościowe; o otwarcie lokaty; o ustalenie limitu na koncie; o pożyczkę; o kontakt z banku w sprawie wybranego produktu; o świadczenie Rodzina 500+; o świadczenie Dobry Start);
- obsługa Profilu Zaufanego ePUAP;
- dostęp do ofert produktów i usług oraz komunikatów informacyjnych banku;
- bieżąca komunikacja z bankiem, składanie reklamacji, sugestii, zapytania;
- obsługa funduszy inwestycyjnych;
- możliwość zamówienia gotówki do oddziału w przypadku wypłaty większej kwoty;
- dostęp do historii transakcji.

Zakres oferowanej funkcjonalności oraz stopień ujednolicenia interfejsu użytkownika w aplikacjach bankowości internetowej i mobilnej jest oczywiście charakterystyczny dla rozwiązań oferowanych przez konkretny bank. Należy jednak przyjąć, że aplikacje webowe dla bankowości internetowej i aplikacje mobilne instalowane np. na smartfonach stanowią dwa różne kanały komunikacji z bankiem. Dodatkowo, aplikacje na urządzeniach mobilnych dają klientom możliwość realizacji zbliżeniowych płatności bezgotówkowych.

Na rynku płatności dostępne są obecnie rozwiązania konkurencyjne względem aplikacji webowych i mobilnych oferowanych przez banki. Na uwagę zasługują tutaj systemy Google Pay dla urządzeń działających pod kontrolą systemu operacyjnego Android oraz Apple Pay dla urządzeń działających pod kontrolą systemów operacyjnych Apple MacOS, Apple iOS i Apple iPadOS, a więc nie tylko dla smartfonów, lecz także dla tabletów, smartwatchy czy laptopów. Na fotografii 8 przedstawiono przykładowy widok z aplikacji Google Pay i Apple Pay, działających na smartfonach.



Fotografia 8. Po lewej – aplikacja Google Pay i historia transakcji zrealizowanych za pomocą karty VISA, której dane zostały wprowadzone do aplikacji; po prawej – analogiczna aplikacja Apple Pay, zachęcająca do wprowadzenia danych kart płatniczych, pokładowych, biletów, kuponów itd. w celu rozpoczęcia realizowania zbliżeniowych transakcji bezgotówkowych autoryzowanych biometryczną funkcją rozpoznawania twarzy: Face ID[27]

Obydwa systemy płatności działają na podobnej zasadzie, pozwalając wprowadzić dane wielu kart płatniczych i realizować w wygodny sposób np. zbliżeniowe transakcje bezgotówkowe w punktach handlowo-usługowych, taksówkach, automatach dystrybucyjnych czy sklepach internetowych. Kluczowe jest tutaj spełnienie przez urządzenie – oprócz wymagań dotyczących systemu operacyjnego – takich kryteriów, jak wsparcie dla standardu komunikacji bliskiego zasięgu NFC (ang. *Near-Field Communication*), czy też posiadanie kamery wideo wysokiej rozdzielczości i czytnika linii papilarnych. Rozwiązania Google Pay i Apple Pay pozwalają bowiem na autoryzację transakcji z użyciem metod biometrycznych, takich jak rozpoznawanie twarzy lub odcisku palca użytkownika. Głównym atutem obydwu rozwiązań jest łatwość obsługi i szybkość realizacji zbliżeniowych płatności bezgotówkowych. Kluczowe dla działania usługi i dalszej jej popularyzacji jest jednak wsparcie ze strony banków.

[27] Na podst.: (1) M. Żołyniak, *#wSkrócie: Google Pay już dostępne, ważna zmiana w Androidzie P i nowy test szybkości OnePlusa 5T, https://komorkomania.pl/35661,wskrocie-google-pay-juz-dostepne-wazna-zmiana-w-androidzie-p-i-nowy-test-szybkosci-oneplusa, stan z dn. 3 lipca 2021; (2) K. Duliński, Płatności Apple Pay, https://www.najlepszekonto.pl/apple-pay, stan z dn. 3 lipca 2021.*

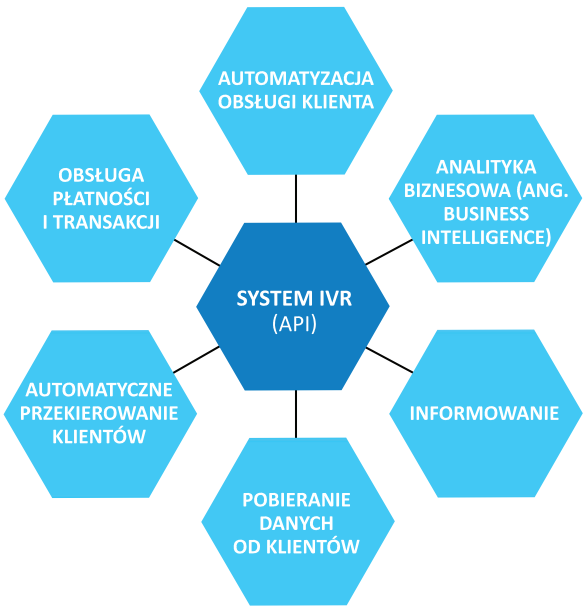
1.6. Rozwiązania oparte o połączenia telefoniczne

Rozwiązania oparte o połączenia telefoniczne to przede wszystkim kontakt telefoniczny z pracownikiem biura obsługi klienta (BOK; ang. *call centre* – centrum obsługi telefonicznej) lub realizowany za pośrednictwem systemu IVR (ang. *Interactive Voice Response* – interaktywne odpowiedzi głosowe), dzięki któremu klient banku może wykonywać podstawowe operacje bankowe i zapoznać się z ofertą usługowo-produktową.

Pierwsze systemy IVR pojawiły się na początku lat 80. XX wieku i stały się popularne w zastosowaniach związanych z rezerwacją biletów lotniczych[28]. Na początku XXI wieku ich możliwości rozszerzono o funkcje związane z automatyzacją obsługi klientów, co sprawiło, że część analityków przewidywała szybki koniec typowych BOK. Tak się jednak nie stało, a systemy IVR są w stanie doskonale uzupełniać i zwiększać możliwości obsługi klientów, działając równolegle do bankowego centrum obsługi telefonicznej, a w szczególnych przypadkach przekierowując połączenie do konsultanta. Potencjał systemu IVR, który współcześnie, dzięki interfejsowi programowania aplikacji (ang. *Application Programming Interface, API*), może być zintegrowany z wieloma innymi systemami i źródłami danych dostępnymi dla banku, jest obecnie jeszcze większy. Na schemacie 2 przedstawiono możliwości integracji przez API i podstawowe funkcje systemu IVR.

W zakresie funkcjonalności system IVR jest w stanie realizować następujące zadania w poszczególnych obszarach:

- Automatyzacja obsługi klienta – np. przekazanie informacji o statusie zamówienia lub zgłoszenia od klienta; przedstawienie salda rachunku bankowego; przypomnienie terminów płatności itp.
- Obsługa płatności i transakcji – np. wspomaganie realizacji opłat; autoryzacja opłat cyklicznych.
- Automatyczne przekierowywanie klientów – np. przekierowanie klienta do odpowiedniego departamentu bankowego na podstawie udzielonych odpowiedzi; przekierowanie klienta w oparciu o reguły związane z kalendarzem i porą doby, kodem pocztowym, danymi globalizacyjnymi czy też na podstawie dotychczasowej wiedzy na temat wyniku poprzedniego połączenia lub posiadanego przez klienta połączenia produktów i usług.
- Pobieranie danych od klientów – np. aktywacja nowych lub wymienionych kart płatniczych; w przypadku konieczności podniesienia poziomu bezpieczeństwa system IVR może przesłać wiadomość tekstową lub połączyć się z klientem w celu przekazania hasła jednorazowego; przeprowadzanie ankiet i sondaży przez telefon;



Schemat 2. Podstawowe funkcje i możliwości integracji systemu IVR za pośrednictwem API

[28] *What is Interactive Voice Response (IVR)?*, https://www.ivrtechgroup.com/ivr/what-is-interactive-voice-response-ivr, stan z dn. 3 lipca 2021.

- Informowanie – np. przekazywanie klientom informacji na temat istotnych zdarzeń (w tym związanych z bezpieczeństwem bankowości); przesyłanie informacji na temat zbliżających się lub przekroczonych terminów opłat;

- Analityka biznesowa – np. zbieranie i analiza informacji pochodzących od różnych grup klientów, z różnych regionów geograficznych itp. celem wykrycia potencjalnych problemów i optymalizacji oferty; zbieranie informacji diagnostycznych w celu ulepszenia komunikacji z klientem; wytyczanie trendów przy użyciu technik wizualizacyjnych z obszaru Big Data.

Wydaje się, że pomimo postępującej transformacji cyfrowej bankowości, uznane od wielu lat formy kontaktu z bankiem, takie jak połączenia z *call center* i wykorzystanie systemów IVR, wciąż będą funkcjonować obok nowych kanałów komunikacji. Ich możliwości będą się zwiększały dzięki postępującej integracji i stosowaniu technologii z obszaru Big Data czy sztucznej inteligencji (np. przetwarzanie języka naturalnego i wykorzystanie tzw. *chatbotów* – automatów dyskusyjnych pozwalających w jeszcze większym stopniu automatyzować proces obsługi klienta).

ROZDZIAŁ II

PROGRAM ANALITYCZNO BADAWCZY

Słabe i silne strony istniejących rozwiązań

Niniejszy rozdział skupia się na słabych (sfera podatności) i mocnych (sfera zabezpieczeń) stronach rozwiązań funkcjonujących w obszarze bankowości elektronicznej – zarówno zabezpieczenia, jak i podatności zostały omówione w dedykowanych podrozdziałach.

Informacje przedstawione w poszczególnych podrozdziałach są wynikiem:

- analizy artykułów naukowych i literatury specjalistycznej dotyczącej omawianego zagadnienia;
- badań terenowych/ankietowych klientów bankowości elektronicznej w celu określenia ich poziomu świadomości i umiejętności korzystania z bankowości elektronicznej;
- wywiadów eksperckich przeprowadzanych z respondentami, którzy reprezentowali środowisko związane z sektorem bankowym, działami bezpieczeństwa i IT instytucji finansowych oraz z biegłymi sądowymi.

2.1. Zabezpieczenia

Z punktu widzenia banku, fundamentalną kwestią w odniesieniu do transakcji realizowanych kartami płatniczymi jest przestrzeganie 12 wymagań zgrupowanych w 6 grup tematycznych (celów kontrolnych) standardu PCI DSS (ang. *Payment Card Industry Data Security Standard*), który zapewnia spójny poziom bezpieczeństwa w instytucjach związanych z przetwarzaniem danych kart płatniczych. Dla poszczególnych celów kontrolnych są to:

I. Zbuduj i utrzymuj bezpieczną sieć:

1. Zainstaluj i utrzymuj odpowiednią konfigurację zapory sieciowej, aby chronić dane posiadaczy kart.
2. Nie używaj domyślnych haseł ani innych parametrów bezpieczeństwa ustawionych przez producentów.

II. Chroń dane posiadaczy kart:

3. Chroń dane posiadaczy kart w trakcie ich przechowywania.
4. Szyfruj transmisję danych posiadaczy kart w otwartych, publicznych sieciach.

III. Prowadź program zarządzania podatnościami:

5. Używaj i regularnie aktualizuj oprogramowanie antywirusowe.
6. Twórz i utrzymuj bezpieczne systemy i aplikacje.

IV. Zaimplementuj silne mechanizmy kontroli dostępu:

7. Ogranicz dostęp do danych posiadaczy kart płatniczych tylko dla osób, które mają taką potrzebę biznesową.
8. Przydziel użytkownikom systemu komputerowego unikalne identyfikatory.
9. Ogranicz fizyczny dostęp do danych posiadaczy kart.

V. Regularnie monitoruj i testuj sieci:

10. Kontroluj i monitoruj cały dostęp do zasobów sieciowych i danych posiadaczy kart.
11. Regularnie testuj systemy i procesy bezpieczeństwa.

VI. Utrzymuj politykę bezpieczeństwa informacji:

12. Utrzymuj politykę, która obejmuje bezpieczeństwo informacji.

Powyższe wymagania mają kluczowe zastosowanie w przypadku urządzeń, aplikacji i transakcji, które opierają się na wykorzystaniu kart płatniczych. Wynika z nich wiele bardziej szczegółowych zaleceń, które pozwalają wdrożyć odpowiedni poziom zabezpieczeń.

Z punktu widzenia klienta nie istnieje żaden zdefiniowany standard dotyczący wymagań bezpieczeństwa bankowości elektronicznej. Klienci muszą tutaj polegać na informacjach przekazywanych głównie przez banki, przy czym należy zauważyć, że w niektórych przypadkach można odnieść wrażenie nadmiaru, co ma negatywny skutek – istotne informacje znikają bowiem w szumie wskazówek, dobrych praktyk, wymagań i ostrzeżeń.

2.1.1. Zabezpieczenia urządzeń

W przypadku urządzeń, które przetwarzają dane kart płatniczych, takich jak: bankomaty, terminale płatnicze (POS) czy bitomaty, istotne jest zabezpieczenie przed tzw. *skimmingiem* – atakiem, który polega na nieautoryzowanym przechwyceniu informacji zapisanych na pasku magnetycznym karty płatniczej poprzez modyfikację sprzętu lub oprogramowania urządzenia płatniczego (np. bankomatu, terminala płatniczego).

Skimming realizowany jest często z użyciem zewnętrznego czytnika kart płatniczych i bywa łączony z kradzieżą numeru PIN, do czego wykorzystuje się nakładki na klawiatury numeryczne lub ukryte mikrokamery. Udany atak tego typu pozwala przestępcom zebrać informacje potrzebne do wyprodukowania fałszywej karty płatniczej.

Skuteczną metodą zmniejszenia ryzyka związanego ze skimmingiem jest implementacja globalnego standardu EMV (nazwa pochodzi od pierwszych liter organizacji – twórców standardu: Europay, MasterCard i Visa), który umożliwia obsługę płatności przy użyciu kart z mikroprocesorem oraz standardu PCI EPP (ang. *Payment Card Industry* – przemysł kart płatniczych; ang. *Encrypting PIN Pad* – szyfrowanie padu PIN) związanego z urządzeniami przetwarzającymi dane z kart płatniczych.

Z punktu widzenia bezpieczeństwa sprzętu, np. bankomatów i sieci bankomatów, kluczowe jest zabezpieczenie przed atakami logicznymi. Tego typu przestępczość stanowi skoordynowany zestaw złośliwych działań mających na celu uzyskanie dostępu do komputera sterującego bankomatu, jego komponentów (np. interfejsów: RS-232, USB, sieci komputerowej itp.) lub sieci, w której działa bankomat. Przejęcie kontroli nad urządzeniem pozwala przestępcom na wypłatę gotówki lub kradzież danych dotyczących np. używanych w urządzeniu kart[29]. Istnieje wiele odmian ataków logicznych, które sprowadzają się do wykorzystania złośliwego oprogramowania, komputerów lub urządzeń typu „czarna skrzynka" podłączanych bezpośrednio do bankomatów lub do sieci, w której funkcjonują bankomaty.

Na ataki logiczne narażone są także terminale POS i bitomaty. Szczególnie bitomaty wymagają większej uwagi rynku w zakresie zabezpieczeń jako urządzenia stosunkowo nowe. Z pewnością można tutaj częściowo skorzystać z dotychczasowych doświadczeń w zakresie zapewniania bezpieczeństwa klasycznym bankomatom.

W trakcie przeprowadzonych wywiadów, eksperci podkreślali zdolność do wykrywania podatności na urządzeniach końcowych, które są wykorzystywane przez klientów bankowości elektronicznej, takich jak: komputer PC, laptop, tablet i – najpopularniejszy – smartfon. W tym obszarze sugerowano dwa rozwiązania.

Pierwsze, to oprogramowanie zabezpieczające, które zainstalowane na urządzeniu końcowym jest w stanie wykryć obecność oprogramowania pozwalającego na zdalny dostęp do pulpitu użytkownika. Co ważne, nie chodzi w tym konkretnym przypadku o wykrywanie wyłącznie złośliwego oprogramowania, a wręcz przeciwnie, istotne jest tutaj wykrywanie typowego oprogramowania narzędziowego, które bywa używane przez przestępców od przejmowania kontroli nad urządzeniem ofiary – np. oprogramowanie typu AnyDesk lub TeamViewer (dostępne dla systemów operacyjnych MS Windows, Android i MacOS). Zdaniem ekspertów, tego typu oprogramowanie zabezpieczające, które powinno być dostarczane przez zewnętrznego dostawcę, a nie przez bank, pozwala skutecznie ograniczyć aktywność sprawców przestępstw. Ma to szczególne znaczenie w przypadku wszelkich oszustw związanych z różnymi wariantami ataku socjotechnicznego, w którym przestępcy podszywają się np. pod pracowników banku, policjantów lub stosują phishing itp., po czym dążą do tego, aby ofiara zainstalowała oprogramowanie pozwalające przejąć sprawcom kontrolę nad jej urządzeniem końcowym w celu wykonania przelewu środków pieniężnych.

Drugie rozwiązanie, które pozwala lepiej zabezpieczyć urządzenia końcowe ofiar, to monitoring behawioralny. Eksperci podkreślają, że istnieją istotne różnice w schemacie zachowania się klienta banku – człowieka, użytkownika bankowości elektronicznej i zautomatyzowanych botów, które mogą być wykorzystywane przez przestępców na przejętym poprzez instalację złośliwego oprogramowania urządzeniu. Tego typu różnice w schematach zachowania można wychwytywać – np. standardowym zachowaniem bota używanego przez przestępców jest natychmiastowa zmiana numeru telefonu do kontaktu po zalogowaniu się do systemu bankowości elektronicznej. Działanie takie pozwala przestępcom przekierować np. SMS-y służące do autoryzacji transakcji w imieniu ofiary. Oprogramowanie zabezpieczające, które zainstalowane na urządzeniu końcowym ofiary monitoruje wszelkie tego typu anomalie, pozwala zwiększyć kontrolę po stronie banku i zmniejszyć skalę nadużyć. Warto podkreślić, że w tym przypadku technologia jest w stanie ochronić klienta nawet przy założeniu jego mniejszej świadomości zagrożeń – budowana jest bowiem faktyczna odporność przed zagrożeniami.

Zdaniem ekspertów, promowane powinny być wszystkie rozwiązania, które wspierają dwuskładnikowe uwierzytelnianie (2FA). Żadne z dotychczas stosowanych rozwiązań, czy to w postaci aplikacji na tablecie, czy na smartfonie, czy też na komputerze, bez drugiego składnika, który jest dostarczany i weryfikowany innym kanałem komunikacyjnym, nie zapewnia bezpieczeństwa.

[29] *Guidance and recommendations regarding logical attacks on ATMs. Mitigating the risk, setting up lines of defence Identifying and responding to logical attacks*, https://www.ncr.com/content/dam/ncrcom/content-type/brochures/EuroPol_Guidance-Recommendations-ATM-logical-attacks.pdf, stan z dn. 31 maja 2021.

Idealnym modelem byłoby logowanie do usługi bankowej z wykorzystaniem tokenów wspierających standard U2F (ang. *Universal 2nd Factor* – uniwersalny drugi składnik), co oznacza, że parametry logowania są wówczas przechowywane na zewnętrznym urządzeniu poza systemem operacyjnym smartfonu. Należy bowiem mieć na uwadze, że smartfon lub samo otoczenie urządzenia mogą być modyfikowane przez przestępców. Oczywiście możemy mieć do czynienia z atakiem *Man-in-the-Middle* (w dosłownym tłumaczeniu: człowiek w środku – atak polegający na podsłuchiwaniu i modyfikowaniu informacji przesyłanych pomiędzy dwoma stronami bez ich wiedzy), kiedy ktoś przejmie kontrolę nad aplikacją działającą w systemie operacyjnym smartfonu i będzie w stanie przekierowywać ruch, a nawet potwierdzenia z wykorzystaniem tokenu. Są to jednak skrajne przypadki i w rzeczywistości trudno przed nimi skutecznie się bronić. Natomiast bardziej zaawansowanym użytkownikom token daje pewność, że nawet jeżeli ktoś przechwyci jedną naszą transakcję, to jednak nie będzie w stanie wykraść danych potrzebnych do logowania, co oznaczałoby przejęcie pełnej kontroli nad aplikacją bankową. W przypadku smartfonów token będzie działał najczęściej przez interfejs zbliżeniowy, czyli NFC (ang. *Near Field Communication* – komunikacja bliskiego zasięgu).

Im więcej komponentów i funkcji realizowanych jest w sprzęcie, tym lepiej, chodzi tutaj np. o możliwość weryfikacji integralności aplikacji poprzez odwołanie się do platformy czy procesorów kryptograficznych. W przypadku smartfonów będzie to TPM (ang. *Trusted Platform Module* – w dosłownym tłumaczeniu: moduł platformy zaufanej; międzynarodowy standard kryptograficznego układu scalonego), który sprawia, że część funkcji kryptograficznych realizowanych jest w urządzeniu. W procesorach kryptograficznych mogą być przechowywane zarówno kody PIN do logowania do urządzenia, bądź też inne elementy, takie jak dane biometryczne, które mogą być wykorzystywane w postaci opcji weryfikacji odcisku palca.

2.1.2. Zabezpieczenia aplikacji

W tej sekcji omówione zostały zabezpieczenia aplikacji webowych i mobilnych, które umożliwiają bezpieczną komunikację klienta z bankiem. Do kluczowych zabezpieczeń zalicza się: uwierzytelnianie wieloskładnikowe; szyfrowanie połączeń internetowych; silne i regularnie zmieniane hasła dostępowe; biometrię; dobre praktyki użycia aplikacji, np. zakaz korzystania z publicznych sieci Wi-Fi, weryfikowanie podejrzanych maili, SMS-ów lub połączeń telefonicznych, pod którymi mogą kryć się przestępcy dokonujący ataku socjotechnicznego.

Dostęp do usług bankowości elektronicznej należy realizować z użyciem aplikacji przygotowywanych przez instytucje bankowe. Rzadziej powinno korzystać się z dostępu za pośrednictwem przeglądarek internetowych, dlatego że istnieje tutaj ryzyko przekierowania na fałszywą stronę, która wygląda tak, jak autentyczna strona danego banku czy serwisu internetowego.

W przypadku smartfonów lub tabletów najlepiej więc korzystać z aplikacji mobilnych, weryfikując, czy dana aplikacja pobierana jest z oficjalnego sklepu dla danej platformy – odpowiednio: dla systemu operacyjnego Android jest to Google Play, a dla systemu operacyjnego iOS jest to Apple Store. Zawsze musimy upewnić się, kto jest wydawcą aplikacji.

Istotne jest, aby aplikacje były weryfikowane przez sklep pod kątem ich integralności i poziomu bezpieczeństwa na danej platformie. Można przyjąć, że te cechy są dobrze realizowane dla platformy iOS. Natomiast w przypadku platformy Android jakość takiej oceny wciąż rośnie i – warto podkreślić – firma Google cały czas inwestuje w jej dalszy rozwój. Weryfikacja integralności aplikacji ma zapewnić, że robią one tylko to, co powinny robić (zamknięta i znana funkcjonalność) i nie są podatne na współczesne, aktualne modele ataków.

Najmniejsze zaufanie należy mieć do aplikacji opublikowanych we własnych repozytoriach należących np. do deweloperów lub dostawców czy też w sklepach należących do stron trzecich. Należy unikać tego typu metod instalacji, nawet jeżeli bank takie rozwiązania proponuje. Nie powinno się instalować aplikacji z takich źródeł również w przypadku, kiedy na urządzeniu mamy już zainstalowaną aplikację bankową pochodzącą z zaufanego źródła (np. sklep Google).

Aplikacja musi pozwalać na dwuskładnikowe uwierzytelnianie, którego dostawcą mogą być platformy Google Authenticator lub Microsoft Authenticator – zdaniem ekspertów są to dwa najlepsze rozwiązania w tym zakresie. Oczywiście banki mogą stosować inne platformy lub wydawać inne rekomendacje w zakresie drugiego składnika uwierzytelniania. Natomiast z pewnością nie jest zalecaną metodą wykorzystywanie do tego celu kodów SMS, które są niestety wciąż popularne w pewnym zakresie wśród instytucji finansowych.

Przestępcy stosują skuteczne metody przejęcia komunikacji z użyciem kanału SMS. Z tego względu w przypadku aplikacji do bankowości elektronicznej – o ile nie rozważamy stosowania platform Google Authenticator lub Microsoft Authenticator – rozsądne wydaje się wykorzystanie biometrii. Rozwiązania pozwalające na biometryczną weryfikację transakcji są nie tylko bezpieczne, lecz także wygodne, co sprawia,

że doskonale wpisują się w oczekiwania klientów (patrz wykresy 19 i 20).

Należy podkreślić słowa jednego z ekspertów, który na podstawie przeprowadzonej obserwacji zauważył, że większość aplikacji bankowych podczas logowania użytkownika ciągle używa tylko kombinacji użytkownik-hasło. Dopiero na poziomie transakcji włączane jest silne uwierzytelnianie (MFA). Tymczasem dane, takie jak dochody, transakcje klienta itp. są stosunkowo łatwo dostępne dla przestępców.

W odniesieniu do zabezpieczeń aplikacji, warto przywołać separację uprawnień w zarządzaniu aplikacją mobilną na smartfonie, która pozwala na dostęp do wrażliwych parametrów, np. limitów transakcyjnych, wyłącznie za pośrednictwem bankowości internetowej (dostępnej z poziomu przeglądarki, np. na notebooku).

Istotnym zabezpieczeniem, które może być kojarzone zarówno z bezpieczeństwem urządzeń, jak i aplikacji mobilnych, używanych do bankowości elektronicznej, jest wymuszanie odblokowania ekranu urządzenia. Eksperci podkreślali, że jest to warunek podstawowy przed dokonaniem płatności zbliżeniowej aplikacją mobilną. Ekran odblokowywany powinien być za pomocą kodu PIN lub odcisku palca. Dodatkowo, w przypadku, kiedy urządzenie nie posiada aktywnej blokady ekranu, aplikacja mobilna do płatności elektronicznych nie powinna w ogóle działać. Zwracano uwagę, że w takim kierunku idzie dostawca systemu płatności BLIK.

2.1.3. Zabezpieczenia transakcji

Wśród znanych – do tej pory – metod zabezpieczania transakcji wymienić należy narzędzia autoryzacyjne, takie jak kody SMS, tokeny mobilne, tokeny sprzętowe (fizyczne), listy kodów jednorazowych (tzw. zdrapki), rejestrację urządzeń używanych do bankowości mobilnej, określanie limitów wartości transakcji, określanie dziennych limitów transakcji mobilnych, kody PIN, kody QR, podpis elektroniczny[30].

Istotne jest tutaj kryterium zgodności z dyrektywą PSD2 (ang. *Payment Services Directive*)[31], która weszła w życie w dniu 13 stycznia 2016 r., a także z wprowadzonym przez nią wymaganiem silnego uwierzytelniania – SCA (ang. *Strong Customer Authentication*). Wymóg ten oznacza, że tożsamość użytkownika usług płatniczych powinna być weryfikowana z wykorzystaniem przynajmniej dwóch składników.

W przypadku transakcji online typu *card not present,* czyli wykonywanych bez fizycznego użycia karty płatniczej w Internecie, warto wyróżnić – obok standardowych zabezpieczeń – polegających na podaniu danych karty – protokół 3-D Secure, który wprowadza dodatkową warstwę bezpieczeństwa. Oznacza to, że każda tego typu transakcja będzie wiązała się z koniecznością dodatkowej autoryzacji przy użyciu jednego z elementów zapewniających silne uwierzytelnianie. Daje to większą pewność, że transakcja autoryzowana jest przez faktycznego właściciela karty, szczególnie w przypadku jej kradzieży.

Eksperci krytykowali stosowane do dziś silne uwierzytelnianie transakcji za pośrednictwem kanału SMS. Podstawowym zarzutem była tutaj popularność ataku *SIM swap*, który polega na skopiowaniu karty SIM ofiary, co pozwala przestępcom silnie uwierzytelniać (czy raczej autoryzować) transakcje w imieniu ofiar. W związku z tym zalecali, aby zamiast kodów SMS, używać innej metody potwierdzania tożsamości, która powinna funkcjonować w oddzielnym kanale – w optymalnym scenariuszu, jeżeli na jednym urządzeniu dokonujemy operacji, to na drugim urządzeniu powinniśmy potwierdzać nasze operacje. Dobrym rozwiązaniem, które powinno wyprzeć kody SMS, może być zastosowanie aplikacji mobilnej i uwierzytelniania z wykorzystaniem biometrii. Proces powinien być tutaj kontrolowany przez dostawcę urządzenia lub dostawcę aplikacji, czyli przez bank. Alternatywą dla kodów SMS i biometrii, która dostępna jest już dziś i nie generuje większych kosztów, są aplikacje uwierzytelniające Google Authenticator lub Microsoft Authenticator, które mogą generować kody jednorazowe dla określonej transakcji.

2.2. Podatności

W tym podrozdziale opisane zostały podatności, czyli słabe strony rozwiązań dostępnych dla klientów bankowości elektronicznej. Mają one wymiar zarówno techniczny (np. luki w zabezpieczeniach sprzętu lub aplikacji, umożliwiające przeprowadzenie udanego ataku), jak i ludzki (dotyczą sfery ludzkiej psychiki i emocji).

Obydwa rodzaje podatności – techniczne i ludzkie – mogą być z powodzeniem wykorzystywane w działalności przestępczej skierowanej przeciwko klientom bankowości elektronicznej.

[30] A. Gil, K. Senderecki, *Mechanizmy zabezpieczania transakcji elektronicznych, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa", 2016, t. IV, s. 156-158.*

[31] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015L2366&from=PL, stan z dn. 1 czerwca 2021.

Niektórzy eksperci podkreślali fakt, że banki skupiają się na przekazywaniu informacji i wymagań odnośnie bezpieczeństwa do klientów, co sprowadza się często do przerzucania na nich odpowiedzialności za pełne zrozumienie informacji i spełnienie wymagań. Dzięki temu budowana jest świadomość zagrożeń po stronie klientów, ale nie oznacza to, że w ślad za tą świadomością powstaje jakakolwiek odporność (w rezultacie klienci wiedzą, co mają robić i czego unikać, ale nie wiedzą jak). Z tego powodu wiele podatności może być z powodzeniem wykorzystanych przez przestępców – klienci bowiem, chociaż są w stanie wyliczyć różnego rodzaju zagrożenia, nie wiedzą w rzeczywistości, jak się przed nimi bronić i w efekcie stają się podatni na oddziaływanie przestępcze.

Część ekspertów zwracała uwagę, że banki po swojej stronie nie podejmują odpowiedniej liczby działań mających na celu przygotowanie dla klientów rozwiązań w zakresie bezpieczeństwa, które będą dla nich w pełni zrozumiałe, jeżeli chodzi o celowość ich stosowania. Wyklucza to świadomą zgodę klientów na stosowanie tychże rozwiązań i sprzyja poszukiwaniu obejść. Jest to istotny obszar powstawania podatności.

2.2.1. Podatności urządzeń

Ciągłe zagrożenie skimmingiem wynika bezpośrednio z faktu, że nie wszystkie terminale płatnicze (POS) i bankomaty w Europie wyposażone są w niezbędne zabezpieczenia antyskimmingowe. Umożliwia to przestępcom kopiowanie danych z paska magnetycznego kart płatniczych w terminalach POS i bankomatach, co nadal jest dominującym rodzajem oszustwa w Europie. Jest tak, pomimo faktu, że późniejsze wykorzystanie sklonowanej karty płatniczej z paskiem magnetycznym jest prawie niemożliwe na terenie Europy, ponieważ powszechnie stosowane są tutaj karty mikroprocesorowe Europay, MasterCard i Visa (standard EMV). Na poziomie globalnym sytuacja jest jednak inna, zwłaszcza w przypadku krajów, które jeszcze nie dostosowały się do wymagań standardu EMV. W rezultacie wypłata środków z użyciem podrobionej karty wyposażonej w pasek magnetyczny możliwa jest na terenie takich właśnie państw, co ostatecznie stanowi poważny problem dla europejskich wydawców kart płatniczych[32].

W przypadku urządzeń, z których korzystamy na co dzień, typowe są podatności dla smartfonów, np. kwestia, z jakiej wersji systemu operacyjnego Android dana platforma sprzętowa korzysta i czy jest regularnie aktualizowana, jeżeli chodzi o wersję systemu operacyjnego. Warto podkreślić, że dla systemu operacyjnego Android wsparcie jest dość ograniczone, a jego okres to mniej więcej rok. Niektórzy producenci, np. Samsung, oferują dużo dłuższy okres aktualizacji.

2.2.2. Podatności aplikacji

Oprócz aktualizacji systemu operacyjnego danego urządzenia, istotne są aktualizacje samej aplikacji, a więc ważne jest to, aby dostępność tego typu aktualizacji sprawdzać i regularnie je instalować. Zwykle bowiem aktualizacja aplikacji jest powiązana z faktem, że znalezione zostały podatności w systemie operacyjnym, w którym zainstalowane są te aplikacje.

Najczęstszą podatnością jest więc to, że aplikacje nie są aktualizowane, bądź zostały przygotowane bez uwzględnienia metodologii i aktualnego modelu zagrożeń.

Pośród innych podatności wskazano luzowanie reguł bezpieczeństwa, np. rezygnację z SCA (ang. *Strong Customer Authentication* – silne uwierzytelnianie klienta), co w przypadku mniej świadomych użytkowników stwarza wysokie ryzyko oraz możliwość dokonywania zakupu bez potwierdzania kodem BLIK np. w tzw. zaufanych sklepach.

2.2.3. Podatności transakcji

Główną podatnością są jakiekolwiek transakcje wykonywane z wykorzystaniem połączenia telefonicznego. Eksperci podkreślali istnienie podatności – zarówno po stronie klientów, jak i pracowników banków – związanej z atakami przeprowadzanymi za pomocą techniki zwanej „vishing" (od ang. *voice* i *phishing* – co oznacza odmianę ataku socjotechnicznego typu *phishing*, ale realizowaną za pomocą połączenia głosowego, np. telefonicznego).

Istnieje bowiem ryzyko, że przestępcy będą korzystać z numeru bardzo zbliżonego lub wręcz pokrywającego się z numerem banku. Wówczas ofiara, z którą nawiązane zostanie połączenie telefoniczne, może przyjąć, że ma kontakt z prawdziwym przedstawicielem banku i podporządkować się poleceniom wydawanym przez przestępców. Warto tutaj przywołać wyniki ankiety, w której większość respondentów we wszystkich grupach wiekowych wskazywała telefon jako preferowany kanał komunikacji z bankiem (patrz wykresy 6 i 7 w dalszej części opracowania). Istotny jest także wniosek przedstawiony przez ekspertów, którzy zauważyli, że wysoki poziom świadomości zagrożenia związanego z możliwością kontaktu ze strony fałszywych pracowników banku (patrz wykres 37 w dalszej części opracowania) nie przekłada się na realną odporność potencjalnych ofiar – klientów i pracowników banków.

[32] Internet Organised Crime Threat Assessment (IOCTA) 2019, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, s. 38, stan z dn. 27 lipca 2021.

Najbardziej popularnym działaniem, które podpowiada się tutaj klientom, jest przerwanie każdej rozmowy, która wydaje im się podejrzana. Wówczas najlepszym krokiem jest – o ile to możliwe – udanie się do placówki bankowej w celu potwierdzenia potrzeby kontaktu lub użycie dowolnego innego kanału komunikacyjnego, poza zwrotnym połączeniem telefonicznym.

Wspomniana podatność dotycząca ludzkiej percepcji jest bowiem ściśle powiązana z podatnością systemów VoIP (ang. *Voice over IP* – systemy połączeń głosowych, które do transmisji wykorzystują sieci IP), które mogą być atakowane przez przestępców w celu przekierowania połączeń. Dotyczy to systemów VoIP działających zarówno po stronie banku (wówczas przekierowywane mogą być połączenia przychodzące), jak i tych, które działają po stronie klienta. W takim przypadku ofiara nie ma praktycznie szans na weryfikację tożsamości dzwoniącego, o ile próbuje tego dokonać za pośrednictwem zwrotnego połączenia telefonicznego.

W korzystnym scenariuszu, kiedy połączenie zwrotne nie zostanie przekierowane przez przestępców, klient dodzwoni się do banku i będzie mógł potwierdzić, czy miał do czynienia z pracownikiem banku. Problematyczne będzie jednak ustalenie – na co zwracali uwagę niektórzy eksperci – czego miał dotyczyć ten pierwotny kontakt.

Kolejna podatność dotycząca transakcji i leżąca w obszarze socjotechniki związana jest z komunikacją przez SMS. Eksperci podkreślali, że klienci z łatwością poddają się manipulacji, a przede wszystkim nie czytają dokładnie treści komunikatów SMS. W związku z tym zdarza się, że w rozumieniu dyrektywy PSD2 silnie uwierzytelniają transakcję, która później jest przez nich kwestionowana. Niektórzy eksperci zwracali w tym kontekście uwagę na przynajmniej częściową odpowiedzialność samych banków, które wysyłają za pomocą SMS treści niepełne, nieprecyzyjne, a czasami zupełnie nieprzydatne, przyzwyczajając użytkowników do tego, aby traktować je pobieżnie. Problemem jest także wysyłanie komunikatów SMS z niewskazanych klientom numerów i bramek.

2.2.4. Podatności infrastruktury

DNS (ang. *Domain Name System* – system nazw domen) nie ma wbudowanych żadnych mechanizmów potwierdzających prawdziwość otrzymanych odpowiedzi. DNSSEC (ang. *Domain Name System Security Extensions* – rozszerzenia bezpieczeństwa systemu nazw domen), pomimo że – na co wskazał jeden z ekspertów – posiada już przestarzałe i niesprawne mechanizmy zabezpieczeń, daje nam możliwość weryfikacji otrzymanych z DNS odpowiedzi. Do tego celu wykorzystywany jest podpis elektroniczny. Co prawda nie zapewnia to prywatności, ale gwarantuje integralność odpowiedzi.

Niestety utrzymanie DNSSEC wymaga dużych nakładów pracy związanych z utrzymaniem, o ile bank nie posiada własnych skryptów lub nie wdroży rozwiązania, takiego jak np. Infoblox. Z tego względu, pomimo tego, że domeny pl i gov.pl są zarejestrowane w DNSSEC przez NASK, większość banków – i szerzej instytucji finansowych – rezygnuje z tego zabezpieczenia. Dodatkowo wsparcie DNSSEC przez dostawców oprogramowania, takich jak Microsoft czy Apple, jest bardzo słabe, albo nawet żadne. Być może przyczyną tego stanu rzeczy jest fakt, że zabezpieczenia kryptograficzne DNSSEC są słabe. Należy jednak podkreślić, że obecnie jest to jedyna możliwość zapewnienia integralności odpowiedzi DNS, co stanowi istotne zabezpieczenie techniczne przed phishingiem. Zabezpieczenia kryptograficzne będące w tej chwili najlepszą alternatywą to funkcje eliptyczne, które dają szybkość działania i większe bezpieczeństwo przy mniejszej długości klucza. Klucze bazowe to wciąż standard RSA.

Eksperci zwrócili również uwagę na podatności sieci radiowych i protokołu SSL/TLS (ang. *Secure Socket Layer/Transport Layer Security* – dosł. warstwa bezpiecznych gniazd/bezpieczeństwo warstwy transportowej). Jedną ze zmian wprowadzonych w sieciach radiowych zabezpieczeniami WPA-3 (ang. *Wi-Fi Protected Access* – chroniony dostęp do Wi-Fi) jest metoda uwierzytelniania SAE (ang. *Simultaneous Authentication of Equals*). SAE jest wariantem wymiany kluczy Dragonfly zdefiniowanej w RFC 7664 i opartej na wymianie kluczy Diffie-Hellman przy użyciu skończonych grup cyklicznych, które mogą być podstawową grupą cykliczną lub krzywą eliptyczną. Generalnie adresuje to problem znany już z IPSec (ang. *Internet Protocol Security* – bezpieczeństwo protokołu internetowego) zwany PFS (ang. *Perfect Forward Secrecy*). Wadą dotychczasowych sieci było bowiem to, że podsłuchanie ruchu radiowego umożliwiało przejęcie materiału klucza, a tym samym złamanie hasła.

Podobny problem występuje w protokole SSL/TLS. Oryginalna specyfikacja chroni początkową komunikację/negocjację kluczy sesyjnych tylko poprzez wykorzystanie klucza publicznego serwera. Kompromitacja klucza prywatnego serwera prowadzi do ujawnienia wszystkich danych klientów serwisu. Rozwiązaniem jest oczywiście generacja kluczy tymczasowych („ulotnych") obowiązujących tylko w ramach sesji. Kompromitacja prywatnego certyfikatu serwera nie daje dostępu do danych sesji – wymaga od atakującego złamania klucza sesyjnego. Z tego względu zalecana jest migracja do TLS 1.3.

2.2.5. Przykłady przełamania zabezpieczeń

Na podstawie wywiadów, które przeprowadzono z ekspertami, można postawić wniosek, że dominują ataki socjotechniczne. Biorąc bowiem pod uwagę zabezpieczenia stosowane przez banki, stosunkowo rzadko zdarzają się próby ataków bezpośrednio na systemy teleinformatyczne.

Najczęściej obserwuje się obecnie próby przekonania drugiej strony, czyli odbiorców (klientów), do tego, aby zainstalowali sugerowaną (przez przestępców) aplikację. Zwykle przestępcy dzwonią do klientów bankowości elektronicznej informując ich o tym, że wykryto atak na ich konto i że za chwilę zadzwoni policjant, który prowadzi postępowanie w tej sprawie. Po chwili, rzeczywiście, następuje kolejne połączenie, napastnik przedstawia się jako policjant, podaje numer służbowy, mówi o tym, że zbierane są dowody, chodzi o diagnostykę zdarzenia i prosi o instalację aplikacji. Podawany jest adres, który należy wprowadzić, pobierana jest aplikacja, a jej instalacja powoduje przejęcie kontroli nad urządzeniem ofiary – w szczególności chodzi tutaj o smartfony czy komputery PC. Nie musi być to aplikacja, którą należałoby sklasyfikować jako złośliwe oprogramowanie (ang. *malware*) – bardzo często ofiary proszone są o instalację typowego oprogramowania narzędziowego, które służy do zdalnej administracji urządzeniami (np. oprogramowanie typu AnyDesk lub TeamViewer dla systemów operacyjnych Google Android, Microsoft Windows i Apple iOS).

Swego czasu bardzo popularne były ataki oparte na klonowaniu kart SIM (ataki typu *SIM swap*). Tak wykonane kopie kart SIM wykorzystywane były do przechwytywania kodów jednorazowych. Jeżeli atakujący był w stanie ukraść komuś lub skopiować kartę SIM i uruchomić ją w systemie, to w tym momencie odbierał potwierdzenia i kody jednorazowe, których mógł użyć do potwierdzenia transakcji. Zdaniem niektórych ekspertów tego typu podatność należy nadal brać pod uwagę – w szczególności, jeżeli chodzi o wykorzystanie komunikacji z użyciem SMS.

Ponadto istotne są próby odgadnięcia haseł. Często identyczne lub zbliżone hasła i identyfikatory są wykorzystywane przez użytkowników w wielu serwisach internetowych. Z tego powodu przy wyciekach dużych zbiorów danych zawierających identyfikatory, adresy email, hasła itp., przestępcy próbują logować się z ich użyciem do różnego typu serwisów internetowych i sprawdzają, czy kombinacje haseł i identyfikatorów zadziałają. Oczywiście w przypadku wykorzystania MFA (ang. *Multi Factor Authentication* – uwierzytelnianie wieloskładnikowe), użytkownik otrzyma informację o tym, że ktoś, gdzieś próbuje zalogować się na jego konto. To powinno wzbudzić alarm, ale istnieje najgorsza możliwość, że użytkownik potwierdzi, iż to rzeczywiście on loguje się na swoje konto, chociaż tego nie robi – wówczas oddaje napastnikom pełną kontrolę nad swoim kontem. Z punktu widzenia przestępców takie działanie może się więc opłacić – szczególnie, jeżeli może zostać zautomatyzowane i przeprowadzone na szeroką skalę (wystarczy, aby atak udał się w jednej na wiele zautomatyzowanych prób).

Bardzo interesującą obserwacją, jeżeli chodzi o przykłady przełamania zabezpieczeń, jest fakt, że pojawiają się transakcje, które są popełniane w sposób świadomy. W typowym scenariuszu ofiara zmanipulowana przez przestępców, którzy podszywają się pod np. doradców finansowych i gwarantują szybki zysk związany z obrotem kryptowalutami, dokonuje transakcji i autoryzuje ją. W takim przypadku, nawet kiedy bank kontaktuje się z ofiarą i próbuje odwieść ją od autoryzacji transferu środków na portfel elektroniczny giełdy kryptowalutowej, sugerując, że może tutaj zachodzić wyłudzenie, ofiara pozostaje pod wpływem przestępców i odrzuca informacje przekazywane przez bank. W rezultacie ofiara dokonuje przelewu, który kwestionuje dopiero w momencie, kiedy okazuje się, że transakcja przyniosła jej stratę. Zwykle ofiary popełniają tutaj cały szereg błędów: potwierdzają SMS-y autoryzacyjne, oddają kontrolę nad swoim urządzeniem instalując oprogramowanie do zdalnej administracji (np. typu AnyDesk lub TeamViewer) i kolejno autoryzują wszelkie operacje wykonywane na koncie bankowym przez lub na rzecz przestępców, włączając podpięcie nowego urządzenia do usług bankowości elektronicznej, co w efekcie sprawia, że przestępcy uzyskują pełną swobodę działania. Należy podkreślić, że odpowiedzialność za skutki tego typu działań leży całkowicie po stronie pokrzywdzonego.

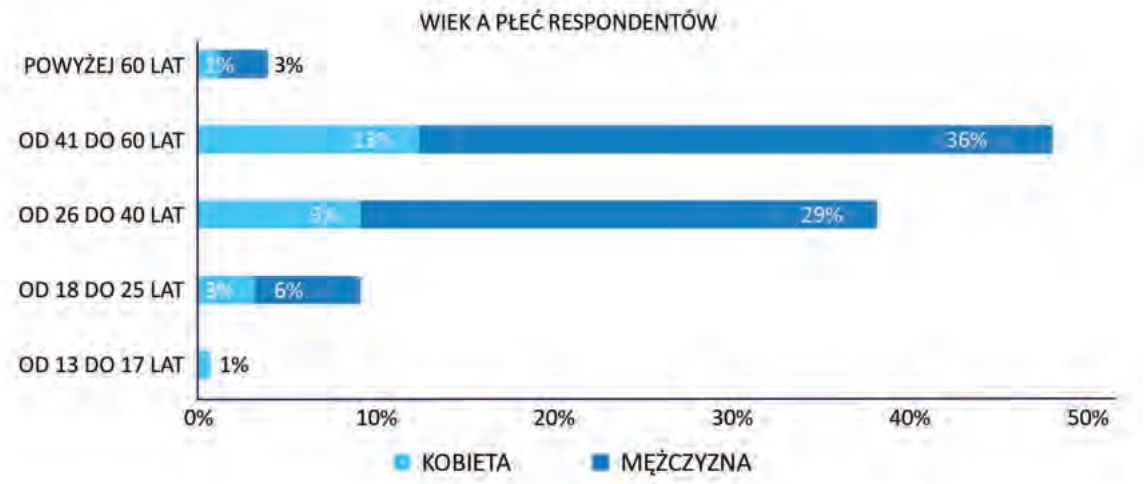
Reasumując, należy stwierdzić, że świadomość klientów bankowości elektronicznej rośnie wraz z ilością ataków i liczbą osób, które w ich otoczeniu padły ofiarą oszustwa. Przede wszystkim chodzi tutaj o oszustwa bezpośrednie, związane z podszywaniem się, czyli *spoofing* i użycie metod socjotechnicznych, a także wykorzystanie podstawionych domen lub witryn, które podszywają się pod domeny lub witryny autentycznych serwisów internetowych i działają jako element pośredniczący w kradzieży danych dostępowych.

ROZDZIAŁ III

PROGRAM ANALITYCZNO BADAWCZY

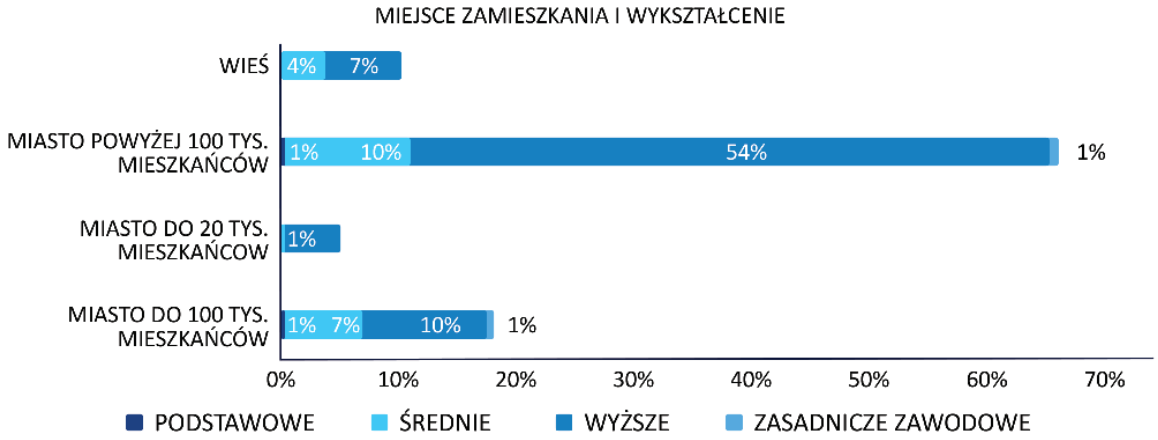
Środowisko bezpieczeństwa klienta bankowości elektronicznej

Na potrzeby niniejszego raportu przeprowadzono badania ankietowe, którymi objęto populację kobiet i mężczyzn – reprezentujących klientów bankowości elektronicznej – w poszczególnych grupach wiekowych: od 13 do 17 lat; od 18 do 25 lat; od 26 do 40 lat; od 41 do 60 lat; powyżej 60 lat (patrz wykres 4). Dominującą grupą klientów bankowości elektronicznej okazali się mężczyźni w wieku od 41 do 60 lat, w drugiej kolejności mężczyźni w wieku 26 do 40 lat. Również pośród kobiet przewagę uzyskała grupa wiekowa od 41 do 60 lat, a na drugim miejscu uplasowała się grupa wiekowa od 26 do 40 lat.



Wykres 4. Wiek a płeć respondentów

W badanej grupie respondentów stwierdzono także zależność pomiędzy miejscem zamieszkania i wykształceniem klientów bankowości elektronicznej – zobrazowaną na wykresie 5. We wszystkich branych pod uwagę miejscach zamieszkania przeważającą grupą okazały się osoby z wykształceniem wyższym. W przypadku miast powyżej 100 tys. mieszkańców to przewaga ponad 5-cio krotna (54% respondentów zadeklarowało fakt posiadania wykształcenia wyższego, a 10% średniego), która maleje w przypadku miast do 100 tys. mieszkańców (10% respondentów z wykształceniem wyższym i 7% respondentów z wykształceniem średnim), miast do 20 tys. mieszkańców (5% respondentów z wykształceniem wyższym i 1% respondentów z wykształceniem średnim) oraz wsi (7% respondentów z wykształceniem wyższym i 4% respondentów z wykształceniem średnim).

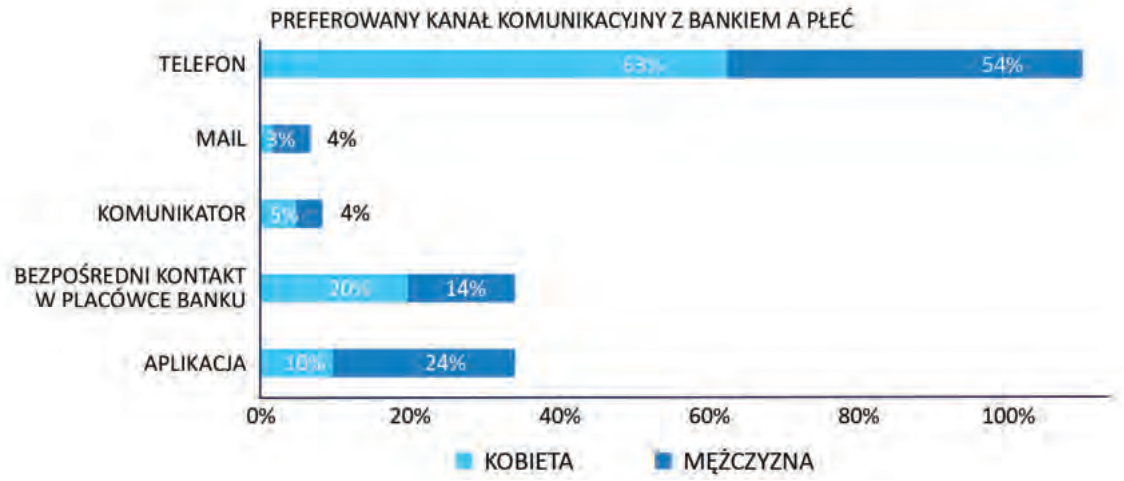


Wykres 5. Miejsce zamieszkania i wykształcenie

Zdaniem niektórych ekspertów, z którymi przeprowadzono wywiady, wyniki przedstawione na wykresie 5 mogą wynikać z faktu, że respondenci mogli wskazywać, iż mieszkają w mieście powyżej 100 tys. mieszkańców, ponieważ z nim się identyfikują z racji wykonywanej pracy, studiowania, spędzania większości czasu. W rzeczywistości, administracyjnie, mogą podlegać pod mniejszy ośrodek (miasto do 20 tys. mieszkańców, miasto do 100 tys. mieszkańców).

3.1. Dojrzałość technologiczna

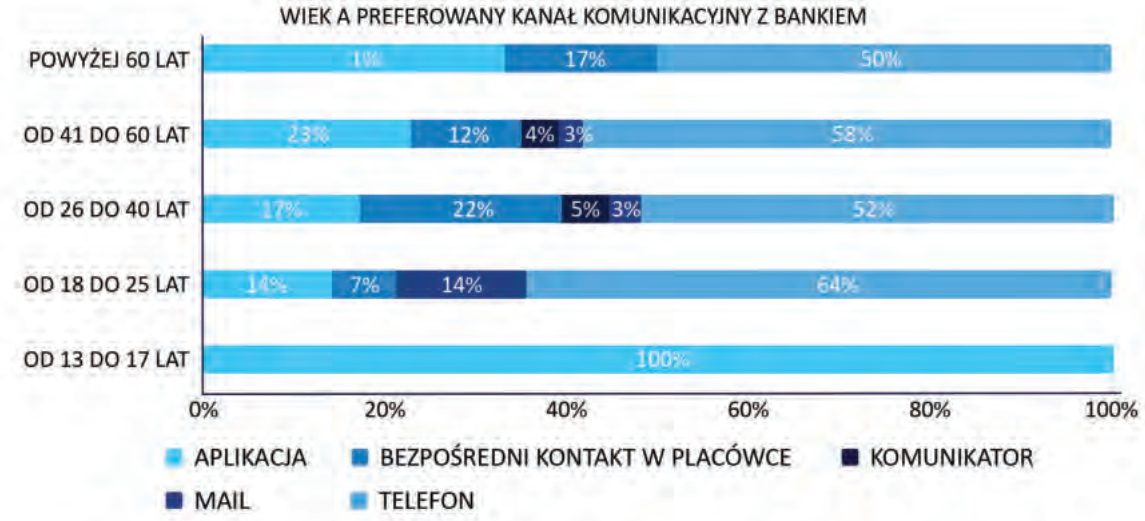
Przeprowadzone badania ankietowe pozwalają dostrzec związek między preferowanym kanałem komunikacyjnym a płcią klienta bankowości elektronicznej (patrz wykres 6). Okazuje się, że w grupie kobiet i mężczyzn najczęściej wybieranym kanałem komunikacji jest telefon (ten kanał wskazało 63% kobiet i 54% mężczyzn). Ciekawie wyglądają preferencje dotyczące bezpośredniego kontaktu w placówce banku i aplikacji: 20% kobiet odpowiedziało, że preferuje bezpośredni kontakt w placówce banku, podczas gdy odpowiedź tą wskazało 14% mężczyzn; jednocześnie 24% mężczyzn wybrało aplikację bankową, jako preferowaną formę komunikacji z bankiem, podczas gdy wśród kobiet było to tylko 10% odpowiedzi. Najmniejszą popularnością w obydwu badanych grupach cieszyły się komunikator (5% kobiet i 4% mężczyzn) oraz mail (3% kobiet i 4% mężczyzn).



Wykres 6. Preferowany kanał komunikacyjny z bankiem a płeć

Uzupełnieniem powyższych obserwacji jest związek pomiędzy wiekiem respondentów a preferowanym kanałem komunikacyjnym z bankiem (patrz wykres 7). W grupach wiekowych od 18 do 25 lat (64% respondentów), od 26 do 40 lat (52% respondentów), od 41 do 60 lat (58% respondentów) i powyżej 60 lat (50% respondentów) dominuje telefon. Na drugim miejscu znajduje się aplikacja wybierana przez 33% respondentów w grupie wiekowej powyżej 60 lat, 23% respondentów w grupie wiekowej od 41 do 60 lat, 17% respondentów w grupie wiekowej od 26 do 40 lat i 14% respondentów w grupie wiekowej od 18 do 25 lat. Wynik 100% w grupie wiekowej od 13 do 17 lat należy uznać za ciekawostkę – nie może być uznany za reprezentatywny ze względu na fakt, że nie zebrano odpowiedniej liczby odpowiedzi, które pozwalałyby potwierdzić tego typu preferencje. Miejsce trzecie, jeżeli chodzi o preferencje respondentów, to bezpośredni kontakt w placówce banku, przy czym jest to kanał komunikacyjny najczęściej wybierany przez osoby w wieku od 26 do 40 lat (22% respondentów), a następnie osoby powyżej 60 lat (17% respondentów) i w grupie wiekowej od 41 do 60 lat (12% respondentów). Pomimo, że bezpośredni kontakt w placówce banku cieszy się najmniejszą popularnością wśród klientów w grupie wiekowej od 18 do 25 lat, to w całościowym ujęciu odpowiedzi przeczą obiegowemu stereotypowi, który głosi, że im starszy klient, tym większe preferencje co do bezpośredniego kontaktu w placówce banku. Można tutaj postawić hipotezę, że rozkład odpowiedzi pomiędzy grupami wiekowymi wynika z faktu, iż grupa wiekowa od 26 do 40 lat podejmuje istotne decyzje związane np. z zaciąganiem kredytów hipotecznych w tym właśnie okresie życia, co przekłada się na preferencje w stosunku do wybieranej wówczas formy komunikacji z bankiem. Jednocześnie w przypadku grupy wiekowej od 18 do 25 lat aż 14% respondentów wskazało mail jako preferowany kanał komunikacji – dla tej grupy wiekowej jest to taka sama liczba odpowiedzi, jak w przypadku aplikacji. W kolejnych grupach wiekowych, czyli od 26 do 40 lat i od 41 do 60 lat mail został wskazany tylko przez 3% odpowiadających. Z kolei preferencje odnośnie użycia komunikatora wskazane zostały wyłącznie przez grupy wiekowe od 26 do 40 lat (5% respondentów) i od 41 do 60 lat (4% respondentów).

Spośród sposobów komunikowania się z bankiem na miejsce pierwsze wysuwa się kontakt telefoniczny, przy czym znamienne jest, iż najmłodsze pokolenie (jako jedyne) preferuje kontakt z wykorzystaniem aplikacji mobilnej. Bardzo interesującym jest, że wraz z wiekiem rośnie poziom zainteresowania wykorzystaniem aplikacji do kontaktów z bankiem i maleje zainteresowanie wykorzystaniem maila jako sposobu



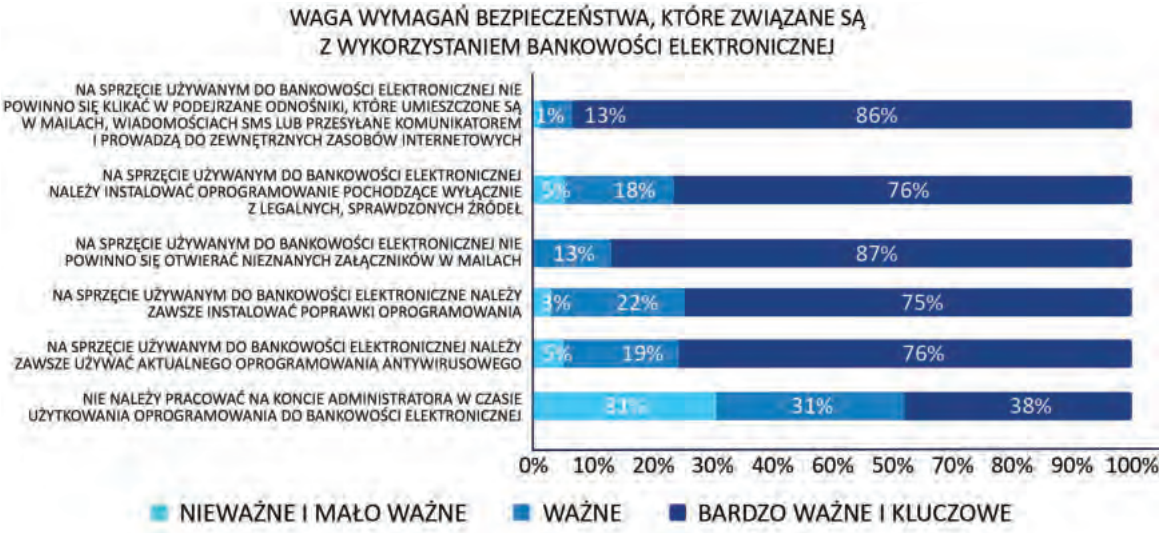
Wykres 7. Wiek a preferowany kanał komunikacyjny z bankiem

komunikowania się. Widać wyraźnie, iż preferowany jest kontakt bezpośredni (on-line lub w placówce banku), zaś komunikacja mailowa schodzi na plan dalszy.

Warto podkreślić, że obecne pokolenie powyżej 60 lat kontakt z bankowością elektroniczną miało już ponad 20 lat temu. Z tego względu ta odmiana bankowości jest przez osoby w tej grupie wiekowej powszechnie używana. Pokolenie, które kategoryzowalibyśmy jako „powyżej 60 lat" w momencie, kiedy bankowość elektroniczna pojawiła się na rynku, dziś powinno być sklasyfikowane jako „powyżej 80 lat". Ludzie Ci mają także całkowicie inne nawyki konsumenckie.

Na wykresie 8 przedstawiono odpowiedzi respondentów, których poproszono o określenie wagi wymagań bezpieczeństwa związanych z wykorzystaniem bankowości elektronicznej. Pomiar ten pozwolił lepiej ustalić poziom dojrzałości technologicznej klientów.

W odniesieniu do wskazań, które diagnozują poziom znajomości zasad higieny i bezpieczeństwa wśród badanych widać, że wskazane w pytaniu podstawowe zasady bezpieczeństwa znajdują silne zrozumienie wśród respondentów. Martwić jednak może, iż zarówno poprawki systemowe, jak i aktualność oprogramowania antywirusowego nie uzyskały zrozumienia i wskazane zostały jako „ważne" przez odpowiednio 22% i 19% respondentów, a jako „bardzo ważne i kluczowe" odpowiednio przez 75% i 76% respondentów. Co więcej, odpowiednio 3% i 5% respondentów określiła je jako „nieważne i mało ważne" – chociaż jest to stosunkowo niski udział procentowy, to zadziwiające może wydawać się, że taka odpowiedź w ogóle była wybierana. W związku z tym, prowadzone na szeroką skalę działania informacyjne w przestrzeni publicznej, jak i samodzielnie przez banki w odniesieniu do klientów bankowości elektronicznej, winny uświadomić potrzebę zabezpieczenia urządzeń poprzez aktualizację



Wykres 8. Waga wymagań bezpieczeństwa, które związane są z wykorzystaniem bankowości elektronicznej

oprogramowania systemowego i antywirusowego w sposób bardziej znaczący i jednoznacznie wpłynąć na rozkład odpowiedzi bardziej w kierunku traktowania tego zagadnienia jako kluczowego z punktu widzenia użytkownika. Jednocześnie eksperci zwracali uwagę, że ciągłe dążenie do korzystania z najnowszej wersji oprogramowania może być problemem – decyzja o aktualizacji musi być świadoma i rozsądna, np.: klient musi rozumieć, że aby korzystać z bankowości elektronicznej będzie musiał wymienić smartfon na nowszy lub pozostanie mu opcja korzystania z dostępu do bankowości elektronicznej przez Internet przy założeniu pewnych kompromisów, ponieważ dalsze wykorzystanie aplikacji mobilnej stanie się niemożliwe na zbyt starym urządzeniu (aplikacja nie będzie działać ze starszą wersją systemu operacyjnego, którego nie można już na danym urządzeniu zaktualizować).

Znamiennym jest także rozkład odpowiedzi na pytanie ostatnie, dotyczące pracy z wykorzystaniem konta administratora – wydawać się może, iż mała znajomość zagadnienia oraz możliwych skutków w przypadku ataku na użytkowany system z wykorzystaniem uprawnień administratora wynika z niewiedzy użytkowników w zakresie możliwej konfiguracji uwzględniającej korzystanie z kont innych aniżeli z uprawnieniami administratora. Odpowiedzi tutaj rozłożyły się dość równomiernie – w odniesieniu do wymagania, które określa, że ze względów bezpieczeństwa nie należy pracować na koncie administratora w czasie użytkowania oprogramowania do bankowości elektronicznej: 31% respondentów uważa, że wymaganie to jest „nieważne i mało ważne"; 31% respondentów stwierdziło, że jest to „ważne" wymaganie; 38% wskazało, że wymaganie to jest „bardzo ważne i kluczowe". Z opinii ekspertów uzyskanych w ramach przeprowadzonych wywiadów wyłania się istotna kwestia w odniesieniu do posiadanej wiedzy użytkowników, a także kierunku, jaki wyznaczyli producenci oprogramowania, a ściślej firma Microsoft. Mianowicie główny użytkownik komputera w ramach systemu MS Windows domyślnie w czasie jego tworzenia posiada przydzielane uprawnienia w grupie administratorów, co przekłada się na poczucie „zwykłego" użytkownika, iż takie rozwiązanie jest optymalne i nie rodzi żadnych zagrożeń. Z odmienną sytuacją mamy do czynienia w systemach linuksowych, gdzie korzystanie z uprawnień administracyjnych jest jawnie deklarowane z linii poleceń („sudo"), zaś zwykły użytkownik nie posiada zbyt dużych uprawnień systemowych.

Z pewnością bardziej pożądaną sytuacją byłoby, gdyby odpowiedź „bardzo ważne i kluczowe" uzyskała więcej wskazań, co przekładałoby się na wniosek odnośnie wysokiej świadomości respondentów co do ról i uprawnień w użytkowych środowiskach.

Eksperci, w toku prowadzonych wywiadów, wskazywali, że dojrzałość bankowości elektronicznej – w powszechnym odbiorze – jest wysoka, czego nie można jednak powiedzieć o dojrzałości jej użytkowników (klientów), jeżeli dojrzałość rozumieć tutaj nie jako świadomość zagrożeń, a realną odporność na nie. Niemniej dynamiczny rozwój technologii sprawia, że z punktu widzenia banków dojrzałość zdaje się rosnąć.

Przestawiono stanowisko, że technologie bankowości elektronicznej są dojrzałe na tyle, na ile banki są konsekwentne w ich wprowadzaniu. Często bowiem banki nie decydują się na wdrożenie dojrzałych rozwiązań dlatego, że koncentrują się na ułatwieniach dla klientów i nie chcą odstraszać ich np. nowymi mechanizmami weryfikacji. W takim przypadku można przyjąć, że jest to nie tyle kwestia braku dojrzałości technologicznej, co braku chęci wprowadzania dojrzałych technologii.

3.2. Procedury bezpieczeństwa

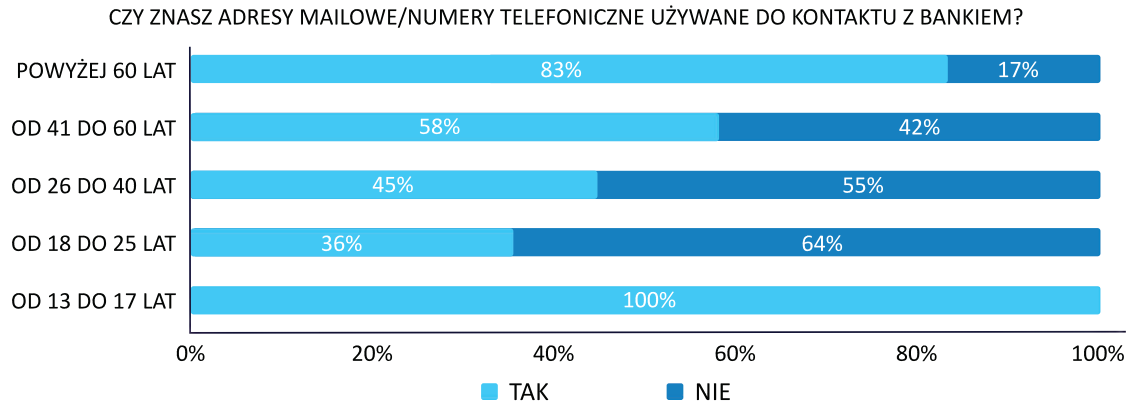
Jedną z podstawowych determinant, która ma wpływ na skuteczną reakcję banku na możliwe zdarzenia, w efekcie których zostanie pokrzywdzony klient bankowości elektronicznej, jest czas, w jakim informacja o zdarzeniu, którą posiada klient, zostanie przekazana do banku. Aby stało się to jak najszybciej, bez zbędnej zwłoki, niezbędnym jest ustanowienie i wykorzystanie kanału szybkiej komunikacji.

Respondenci w ramach badania wskazali, iż posiadają wiedzę jak szybko kontaktować się z bankiem, co świadczy o dobrym przygotowaniu i możliwości reakcji na różnego rodzaju zdarzenia, jakie mogą wpłynąć

Wykres 9. Odpowiedzi na pytanie „Czy wiesz, w jaki sposób szybko kontaktować się z bankiem" w podziale na mężczyzn i kobiety

na bezpieczne funkcjonowanie w środowisku bankowości elektronicznej. Jak wynika z badania, niezależnie od płci, ponad 90% badanych zadeklarowało pełną wiedzę odnośnie szybkiego kontaktu z bankiem (patrz wykres 9).

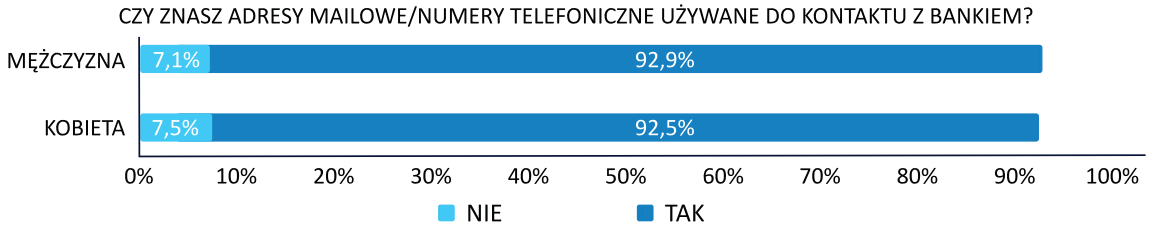
Ciekawym uzupełnieniem powyższych obserwacji jest zestawienie odpowiedzi na pytanie o znajomość adresu mailowego lub numeru telefonicznego używanego do kontaktu z bankiem w poszczególnych grupach wiekowych (patrz wykres 10). Aż 83% respondentów z grupy wiekowej powyżej 60 lat potwierdziło, że zna adres mailowy lub numer telefoniczny używany do kontaktu z bankiem (17% respondentów odpowiedziało przecząco), w kolejnych grupach było to odpowiednio: 68% odpowiedzi twierdzących i 42% odpowiedzi przeczących dla respondentów w grupie wiekowej od 41 do 60 lat; 45% odpowiedzi twierdzących i 55% odpowiedzi przeczących dla respondentów w grupie wiekowej od 26 do 40 lat; 36% odpowiedzi twierdzących i 64% odpowiedzi przeczących dla respondentów w grupie wiekowej od 18 do 25 lat. 100% braku znajomości adresów mailowych lub numerów telefonicznych używanych do kontaktu z bankiem w grupie wiekowej od 13 do 17 lat nie może być traktowany jako wartość reprezentatywna ze względu na zbyt małą liczbę odpowiedzi w tej grupie wiekowej. Jednocześnie należy podkreślić, że w odniesieniu do najmłodszej grupy wiekowej deklarowany brak przekazania informacji wynika prawdopodobnie z faktu, iż kwestie bezpieczeństwa zostały omówione z przedstawicielem ustawowym w momencie zakładania konta i ewentualnie uruchamiania dostępu do systemu bankowego – założenie to można przyjąć także w przypadku odpowiedzi przedstawionych na wykresach 12, 13, 14, 15 i 17.



Wykres 10. Znajomość adresów mailowych lub numerów telefonicznych używanych do kontaktu z bankiem w poszczególnych grupach wiekowych

Bardzo symptomatyczne było zdanie jednego z badanych ekspertów, iż najmłodsza grupa badanych (pokolenie milenialsów) funkcjonuje w sposób odmienny od pokoleń starszych. Pierwsza wskazana różnica to fakt, iż najmłodsze pokolenie nie przywiązuje znaczącej wagi do przekazywanych informacji, zaś druga to fakt, iż najmłodsze pokolenie nie czuje silnych związków z wybranym rozwiązaniem/bankiem i często pod wpływem impulsu go zmienia, zaś od samej zmiany wymagane jest jak najmniejsze obciążenie, zaangażowanie czasu i uwagi, co w efekcie może prowadzić do pominięcia zarejestrowania istotnych kwestii, w tym dotyczących bezpieczeństwa.

Odpowiedzi na to samo pytanie – w zależności od płci respondenta – kształtowały się tak, jak pokazano na wykresie 11. W grupie mężczyzn 92,9% respondentów znało adresy mailowe lub numery telefoniczne



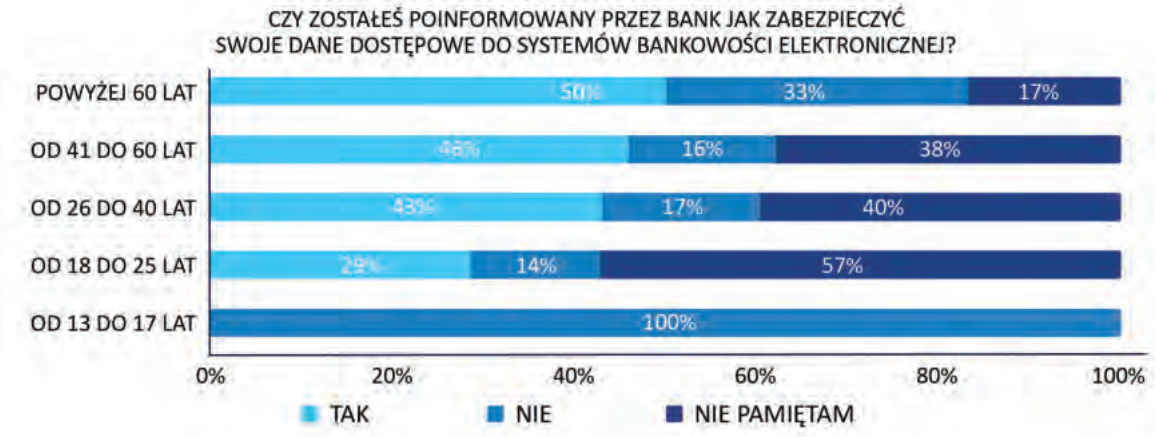
Wykres 11. Znajomość adresów mailowych lub numerów telefonicznych używanych do kontaktu z bankiem w zależności od płci

wykorzystywane do kontaktu z bankiem, a 7,1% odpowiedziało przecząco. W przypadku kobiet 92,5% respondentek zadeklarowało taką znajomość, a 7,5% jej brak.

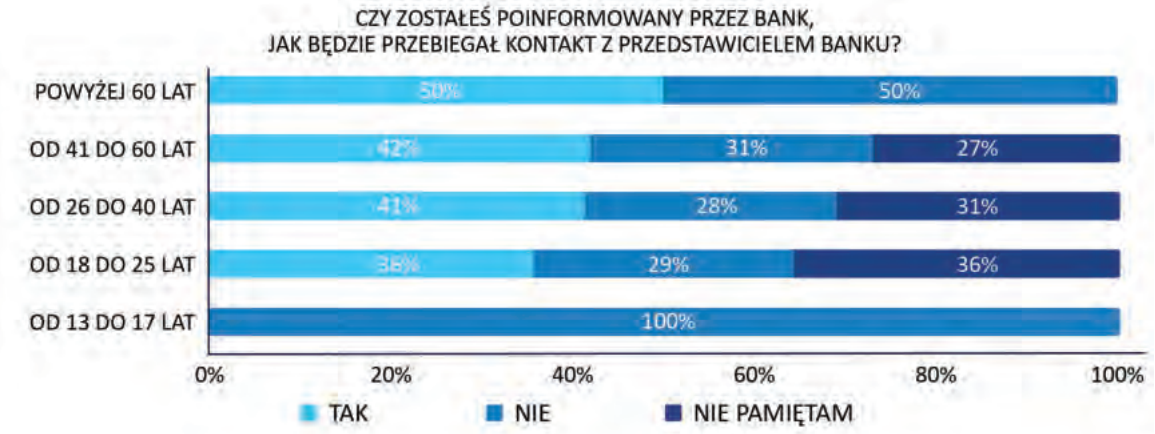
Warto podkreślić, że kontakt telefoniczny jest często wykorzystywanym kanałem komunikacyjnym przez przestępców podszywających się np. pod pracowników banków. Istotnym w tym kontekście jest zagadnienie wiedzy klienta banku odnośnie bezpieczeństwa danych, w tym w szczególności danych osobowych, danych dostępowych i innych, których ujawnienie osobom niepożądanym może narazić ich właściciela na podejmowanie działań przestępczych z ich wykorzystaniem. Znamiennym jest, że wraz z wiekiem rośnie udział osób, które deklarują, że w ramach kontaktu z bankiem przekazana została im informacja, jak zabezpieczyć dane dostępowe do bankowości elektronicznej oraz zostały przekazane informacje, w jaki sposób będzie przebiegała komunikacja z przedstawicielem banku, w tym wiedza nt. ewentualnych danych, które będą wymagane do sprawnej komunikacji (patrz wykres 12, 13). Mając na względzie poprzednie uwagi dotyczące pokolenia milenialsów, osoby młodsze nie przywiązały szczególnej wagi do tego rodzaju informacji i wskazują, iż nie pamiętają, czy bank przekazał im te istotne z punktu bezpieczeństwa informacje.

Wykres 12 przedstawia procentowy udział odpowiedzi na pytanie „Czy zostałeś poinformowany przez bank, jak zabezpieczyć swoje dane dostępowe do systemów bankowości elektronicznej?". Obserwujemy tutaj tą samą prawidłowość, co na wykresie 10, tzn. wraz z wiekiem rośnie udział osób, które deklarują, że posiadają przedmiotową wiedzę. Pojawia się jednak niepewność, która wzrasta wraz z tym, jak obniża się wiek respondentów, a dokładnie: w grupie wiekowej powyżej 60 lat 17% respondentów wybrało odpowiedź „nie pamiętam", 33% odpowiedź „nie", a 50% odpowiedź „tak"; w grupie wiekowej od 41 do 60 lat odpowiedź „nie pamiętam" wskazało już 38% respondentów (ponad dwukrotnie więcej niż w przypadku starszej grupy wiekowej), odpowiedź „nie" wskazało 16%, a odpowiedź „tak" 46%; proporcje w grupie wiekowej od 26 do 40 lat wyglądają podobnie, jak w grupie od 41 do 60 lat, to znaczy, że 40% respondentów odpowiedziało „nie pamiętam", 17% wybrało odpowiedź „nie", a 43% odpowiedź „tak"; w grupie od 18 do 25 lat aż 57% osób wskazało odpowiedź „nie pamiętam", 14% odpowiedź „nie", a 29% odpowiedź „tak"; w najmłodszej grupie wybrano odpowiedź „nie", co wiąże się z faktem, że tego typu informacje są przekazywane przedstawicielom ustawowym.

W przypadku wykresu 13, który obrazuje procentowy udział odpowiedzi na pytanie „Czy zostałeś poinformowany przez bank, jak będzie przebiegał kontakt z przedstawicielem banku?" w podziale na poszczególne grupy wiekowe, obserwujemy dużą liczbę odpowiedzi „nie" i „nie pamiętam". Dla grupy wiekowej powyżej 60 lat podział odpowiedzi „tak" i „nie" wynosi po 50%. W pozostałych grupach wiekowych zmniejsza się liczba odpowiedzi „nie" – dla poszczególnych grup mamy tutaj następujące wyniki: 31% dla grupy wiekowej od 41 do 60 lat; 28% dla grupy wiekowej od 26 do 40 lat; 29% w grupie wiekowej od 18 do 25 lat. Zmniejsza się także liczba odpowiedzi „tak": 42% w grupie wiekowej od 41 do 60 lat; 41% w grupie wiekowej od 26 do 40 lat; 36% w grupie wiekowej od 18 do 25 lat. Pojawia się także istotny element niepewności, który stopniowo wzrasta wraz ze zmniejszaniem się wieku respondentów – odpowiedź „nie pamiętam" wybrało: 27% osób w grupie wiekowej od 41 do 60 lat; 31% osób w grupie wiekowej od 26 do 40 lat; 36% osób w grupie wiekowej od 18 do 25 lat. Zgodnie z przyjętym wcześniej założeniem, w grupie wiekowej od 13 do 17 lat obserwujemy 100% odpowiedzi „nie".



Wykres 12. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank, jak zabezpieczyć swoje dane dostępowe do systemów bankowości elektronicznej?" w podziale na grupy wiekowe

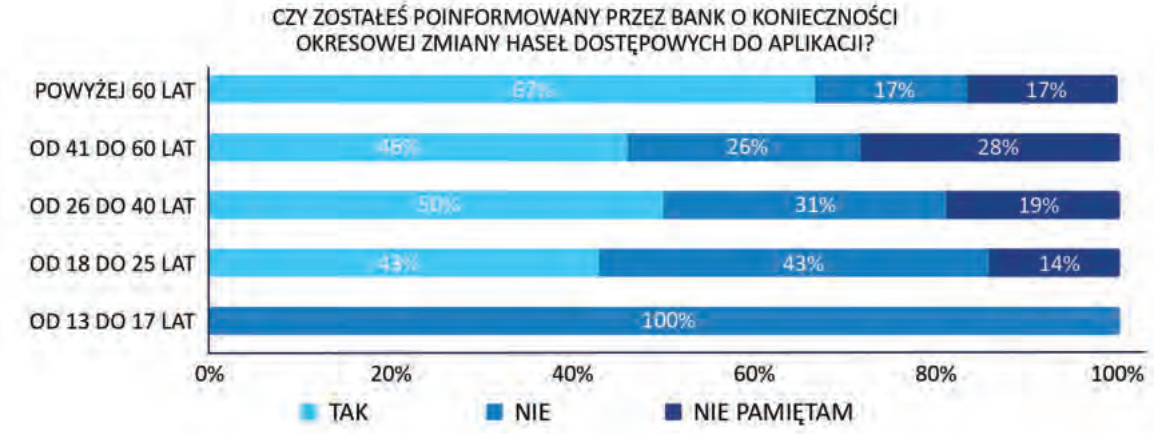


Wykres 13. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank, jak będzie przebiegał kontakt z przedstawicielem banku?" w podziale na grupy wiekowe

Wykres 14 przedstawia odpowiedzi na pytanie „Czy zostałeś poinformowany przez bank o konieczności okresowej zmiany haseł dostępowych do aplikacji?" w poszczególnych grupach wiekowych. Dostrzec można tutaj prawidłowość w grupach wiekowych od 41 do 60 lat, od 26 do 40 lat i od 18 do 25 lat – wraz ze zmniejszaniem się wieku badanych spada tutaj bowiem poziom niepewności, ponieważ w grupie wiekowej od 41 do 60 lat zarejestrowano 28% odpowiedzi „nie pamiętam", w grupie wiekowej od 26 do 40 lat 19% odpowiedzi „nie pamiętam", a w grupie wiekowej od 18 do 25 lat 14% odpowiedzi „nie pamiętam". Jednocześnie w grupach tych wzrasta ilość odpowiedzi „nie" – dla grupy wiekowej od 41 do 60 lat jest to 26% odpowiedzi; dla grupy wiekowej od 26 do 40 lat jest to 31% odpowiedzi; a w grupie wiekowej od 18 do 25 lat jest to aż 43% odpowiedzi. Co ciekawe, to dokładnie tyle samo, ile odpowiedzi „tak" w tej grupie wiekowej i prawie tyle samo, co w grupie wiekowej od 41 do 60 lat, gdzie respondenci odpowiedzieli „tak" w 46% przypadków. Dla porównania, w grupie wiekowej od 26 do 40 lat odpowiedź „tak" została wskazana w 50% przypadków, a w grupie wiekowej powyżej 60 lat aż w 67% przypadków. Trudno więc doszukiwać się tutaj jakiejś prawidłowości, poza obserwacją, że najstarsza grupa wiekowa w istotnym stopniu częściej potwierdzała fakt bycia poinformowanym przez bank na temat konieczności okresowej zmiany haseł dostępowych do aplikacji. Grupa od 13 do 17 lat w 100% odpowiedziała „nie", co jest zgodne z przyjętymi wcześniej założeniami.

Otrzymane na wykresie 14 wyniki są warte szczególnej uwagi, ponieważ dotyczą jednej z podstawowych zasad bezpieczeństwa, a mianowicie konieczności okresowej zmiany haseł dostępowych.

Wyłaniający się zróżnicowany obraz, w którym co prawda w przeważającej części znalazły się odpowiedzi twierdzące (z wyłączeniem najmłodszej grupy) nie może być uznany za satysfakcjonujący w stosunku do wszystkich grup młodszych niż grupa wiekowa powyżej 60 lat, ponieważ ponad jedna trzecia respondentów udzieliła tutaj odpowiedzi przeczącej, a odsetek



Wykres 14. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank o konieczności okresowej zmiany haseł dostępowych do aplikacji?" w podziale na grupy wiekowe

deklarujących brak pamięci odnośnie tej tak istotnej kwestii jest znaczący.

Kwestia bezpieczeństwa urządzeń mobilnych i wykorzystywanych na nich aplikacji mobilnych banku z racji powszechności tego rozwiązania nie może zostać pominięta w rozważaniach na temat środowiska bezpieczeństwa klienta bankowości elektronicznej.

Rozkład odpowiedzi na pytania dotyczące przyjętych powszechnie zasad bezpieczeństwa niestety nie napawa w pełni optymizmem (patrz wykres 15, 16 i 17). Co prawda poziom wykorzystania aplikacji i urządzeń mobilnych jest bezsprzecznie znaczący, lecz deklarowany poziom wiedzy odnośnie tych zagadnień budowany przez bank poprzez indywidualny przekaz informacji odnośnie podstawowych zasad jest – niestety – niski.

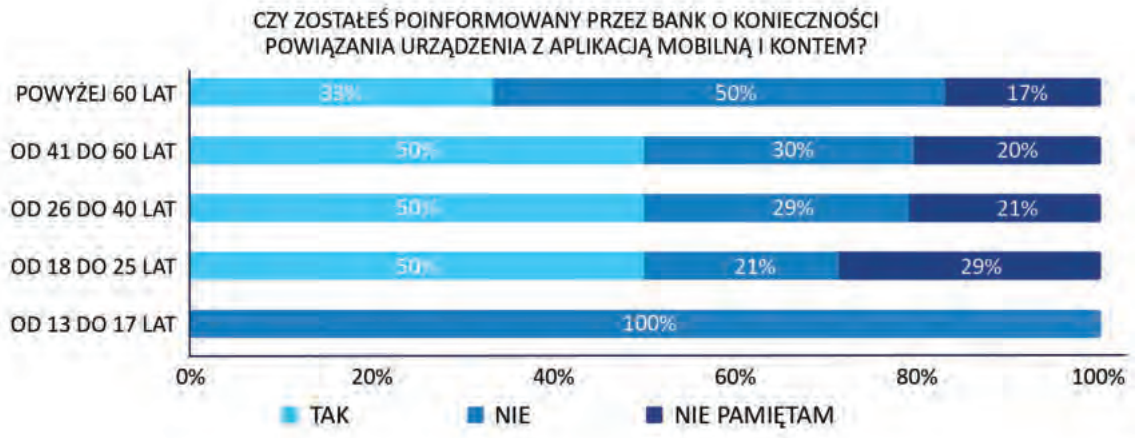
Najwyższy poziom odpowiedzi twierdzących pada na pytanie – „Czy zostałeś poinformowany przez bank o konieczności powiązania urządzenia z aplikacją mobilną i kontem?" (patrz wykres 15). Co prawda sumarycznie 49% respondentów odpowiada na to pytanie twierdząco, jednak przy bliższej analizie zarówno w najmłodszej, jak i najstarszej grupie wiekowej odpowiedź przecząca jest wręcz nieakceptowalna – to odpowiednio: aż 50% odpowiedzi „nie" w grupie wiekowej powyżej 60 lat i 100% odpowiedzi „nie" w grupie wiekowej od 13 do 17 lat. O ile można przywołać wcześniej przyjęte dla najmłodszej grupy wiekowej założenie, że wszelkie informacje od banku przekazywane są do przedstawiciela ustawowego, to mimo wszystko należy podkreślić, że w efekcie ta grupa wiekowa, która w krótkim czasie stanie się pełnoprawnym użytkownikiem bankowości, rozpocznie kolejny etap życia bez koniecznej świadomości odnośnie elementarnych wymagań w obszarze bezpieczeństwa.

Zastanawiający jest także spory udział elementu niepewności w odpowiedziach. Dostrzec można go we wszystkich – poza najmłodszą – badanych grupach wiekowych. W przypadku grupy wiekowej od 18 do 25 lat mamy aż 29% odpowiedzi „nie pamiętam". Następnie w grupie wiekowej od 26 do 40 lat aż 21% respondentów wskazało odpowiedź „nie pamiętam". Na bardzo zbliżonym poziomie znajduje się kolejna grupa wiekowa, od 41 do 60 lat, gdzie odpowiedź „nie pamiętam" wybrało 20% osób. Dla osób powyżej 60 lat odpowiedź „nie pamiętam" stanowi 17% wszystkich odpowiedzi dla tej grupy wiekowej. Widoczny jest więc stopniowy spadek niepewności, w miarę jak wzrasta wiek badanych w grupach wiekowych od 18 do 25 lat aż do grupy wiekowej powyżej 60 lat.

Odwrotną prawidłowość dostrzegamy tutaj dla odpowiedzi „nie" – wraz ze wzrostem wieku badanych, począwszy od grupy wiekowej od 18 do 25 lat, gdzie odpowiedź przeczącą wskazało 21% respondentów, stopniowo wzrasta liczba odpowiedzi przeczących, osiągając kolejno: 29% w grupie wiekowej od 26 do 40 lat; 30% w grupie wiekowej od 41 do 60 lat; aż 50% w grupie wiekowej powyżej 60 lat.

W odniesieniu do pytania dotyczącego zagadnienia konieczności samodzielnego zablokowania urządzenia mobilnego w razie jego utraty (patrz wykres 16) łączny poziom odpowiedzi świadczących o braku otrzymania takiej informacji z banku to ponad 45%. W poszczególnych grupach wiekowych obserwujemy następujące wyniki: 29% odpowiedzi „nie" w grupie wiekowej od 18 do 25 lat; następnie wyraźny wzrost i aż 50% odpowiedzi „nie" w grupach wiekowych od 26 do 40 lat i powyżej 60 lat; oraz zbliżony poziom odpowiedzi „nie" dla grupy wiekowej od 41 do 60 lat, wynoszący 47%.

Element niepewności to aż 43% odpowiedzi „nie pamiętam" w grupie wiekowej od 18 do 25 lat. Następnie wyraźny spadek w grupie wiekowej od 26 do 40 lat, czyli 22% odpowiedzi „nie pamiętam", po którym

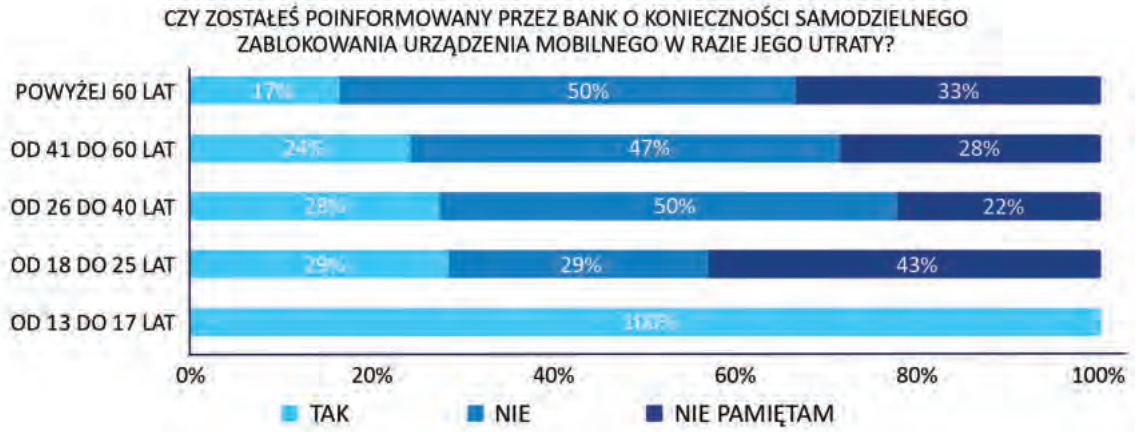


Wykres 15. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank o konieczności powiązania urządzenia z aplikacją mobilną i kontem?" w podziale na grupy wiekowe

można dostrzec stopniowy wzrost dla kolejnych grup wiekowych – odpowiednio: 28% odpowiedzi „nie pamiętam" w grupie wiekowej od 41 do 60 lat; 33% odpowiedzi „nie pamiętam" w grupie wiekowej powyżej 60 lat.

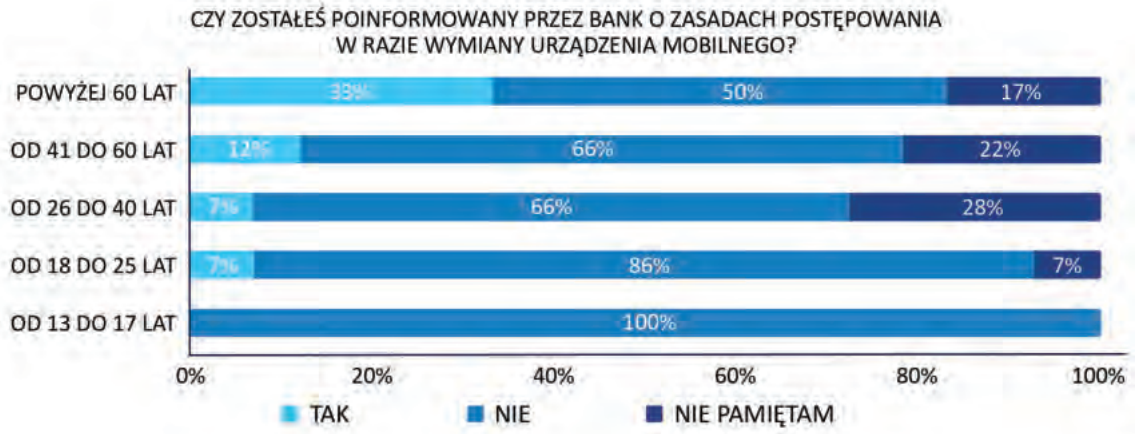
Wyłamuje się tutaj grupa wiekowa od 13 do 17 lat deklarując 100% świadomości odnośnie obowiązku samodzielnego zablokowania urządzenia mobilnego w razie jego utraty. Ze względu na małą liczbę respondentów nie należy tego wyniku przyjmować ze zbyt dużym optymizmem, ponieważ może mieć charakter przypadkowy.

Ogólna ocena wyników przedstawionych na wykresie 16 jest więc negatywna. Oznacza to, że banki muszą upewnić się, że nie tylko przekazują stosowną informację swoim klientom, lecz także upewniają się, iż informacja taka zostanie zapamiętana. Należy przy tym zwrócić uwagę, że jeszcze gorzej sytuacja przedstawia się w odniesieniu do zasad postępowania w razie wymiany urządzenia mobilnego (patrz wykres 17).



Wykres 16. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank o konieczności samodzielnego zablokowania urządzenia mobilnego w razie jego utraty?" w podziale na grupy wiekowe

Wykresy 16 i 17 przedstawiają bardzo trudną sytuację w zakresie wiedzy respondentów, co do zasad postępowania w razie utraty lub wymiany urządzenia mobilnego. W odniesieniu do wykresu 17, który przedstawia odpowiedzi na pytanie „Czy zostałeś poinformowany przez bank o zasadach postępowania w razie wymiany urządzenia mobilnego?", warto podkreślić, że: 100% osób w grupie wiekowej od 13 do 17 lat zadeklarowało odpowiedź „nie" (przypominamy tutaj wcześniejsze założenie, iż tego typu informacje trafiają wyłącznie do przedstawicieli ustawowych); aż 86% respondentów w grupie wiekowej od 18 do 25 lat wybrało odpowiedź „nie", 7% wybrało odpowiedź „tak" i 7% wybrało odpowiedź „nie pamiętam"; 66% osób w grupie wiekowej od 26 do 40 lat odpowiedziało „nie", 28% odpowiedziało „nie pamiętam" i tylko 7% odpowiedziało „tak"; w grupie wiekowej od 41 do 60 lat – podobnie jak w młodszej grupie wiekowej – 66% wskazało odpowiedź „nie", 22% wskazało odpowiedź „nie pamiętam", a 12%



Wykres 17. Odpowiedź na pytanie: „Czy zostałeś poinformowany przez bank o zasadach postępowania w razie wymiany urządzenia mobilnego?" w podziale na grupy wiekowe

wskazało odpowiedź „tak". Najlepiej, chociaż jest to poziom absolutnie niesatysfakcjonujący, wypadła grupa wiekowa powyżej 60 lat, w której – w porównaniu do innych grup: 33% respondentów odpowiedziało „tak" (nadal jest to za mała liczba). Jednocześnie, w tej samej grupie wiekowej, 17% respondentów odpowiedziało „nie pamiętam" i aż 50% respondentów odpowiedziało „nie".

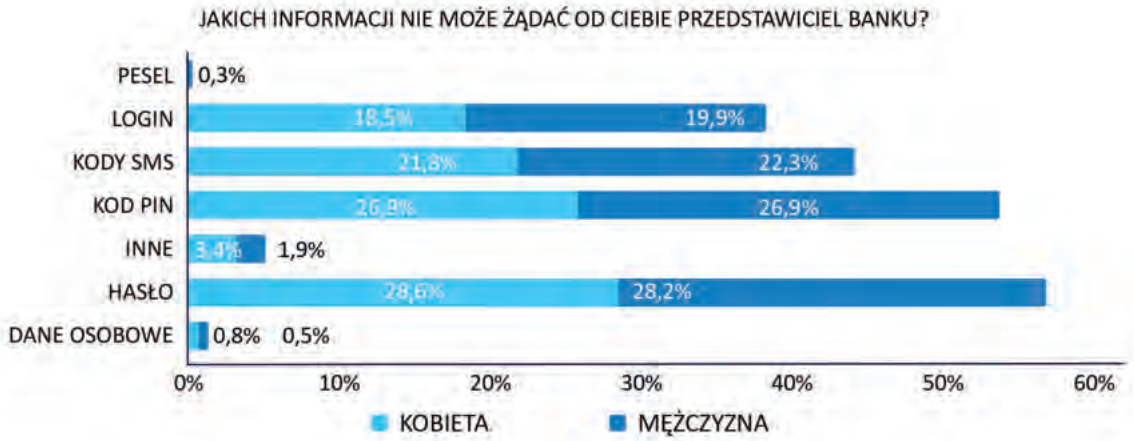
W obszarze związanym ze znajomością procedur bezpieczeństwa istotny jest także poziom wiedzy klientów w zakresie informacji, których nie może żądać przedstawiciel banku. Odpowiedzi na pytanie „jakich informacji nie może żądać do Ciebie przedstawiciel banku?" przedstawiono na wykresie 18.

Respondenci mieli możliwość wskazania dowolnej liczby odpowiedzi wśród zaproponowanych (login, kody SMS, kod PIN, hasło), a dodatkowo mogli podać własne, inne odpowiedzi. W efekcie, co obrazuje wykres 18, odpowiedzi pomiędzy populacją kobiet i mężczyzn rozłożyły się bardzo równomiernie – odpowiednio: 28,9% mężczyzn i kobiet odpowiedziało, że przedstawiciel banku nie może żądać podania kodu PIN; 28,6% kobiet i 28,2% mężczyzn wskazało, że klienta nie można prosić o hasło; 21,8% kobiet i 22,3% mężczyzn wskazało tutaj kody SMS; 18,5% kobiet i 19,9% mężczyzn wybrało login. Tylko 0,3% mężczyzn podało odpowiedź „PESEL". Z kolei 0,8% kobiet i 0,5% mężczyzn podało odpowiedź „dane osobowe", a kategorię inne zaznaczyło odpowiednio 3,4% kobiet i 1,9% mężczyzn.

Eksperci zwracali uwagę, że w powszechnym odczuciu raczej niewielu klientów bankowości w ogóle zapoznaje się z procedurami i niewielu czyta komunikację od banków informującą np. o tym, iż mamy do czynienia z jakimś nowym rodzajem ataków. Wszelkie tego typu informacje są często ignorowane jako element zakłócający dostęp w trybie pilnym do naszych środków płatniczych.

Problem potęgują tutaj nieprofesjonalne biura obsługi klienta (BOK), których pracownicy często są niedostatecznie przeszkoleni, brak im wiedzy, doświadczenia, a w rezultacie często korzystają ze wsparcia II linii. Dostrzega się także wady w skryptach używanych podczas kontaktu z klientem, fakt pojawiania się sztampowych odpowiedzi niepopartych głębszą analizą zgłoszonego problemu.

Odnośnie procedur bezpieczeństwa jeden z ekspertów podkreślił, że jakakolwiek zgoda dotycząca bezpieczeństwa bankowości elektronicznej, którą wyraża klient, powinna być połączona ze świadomością dotyczącą zagrożeń. Przykładowym nieprawidłowym działaniem po stronie banków była sytuacja, w której przesyłano klientom karty zbliżeniowe, nie informując ich, czy są zainteresowani ich użyciem i nie przekazując kompletu informacji o zagrożeniach. W efekcie nie każdy klient miał świadomość, że kradzież karty zbliżeniowej pozwala przestępcom na kradzież części środków pieniężnych (kiedyś do wysokości 50 PLN, obecnie do wysokości 100 PLN) – w przypadku typowej karty płatniczej dostatecznym zabezpieczeniem na okoliczność kradzieży jest kod PIN. W rzeczywistości kwota transakcji zbliżeniowych może przekroczyć limit 50 EUR – co oznacza, że do 50 EUR odpowiadać będzie klient, o ile nie zdążył zastrzec karty, a powyżej limitu 50 EUR odpowiadać będzie dostawca usługi płatniczej. Mieliśmy więc tutaj do czynienia z częściowym przeniesieniem odpowiedzialności za funkcjonalność instrumentu płatniczego z banku na płatnika. Natomiast to bank wygenerował tutaj zagrożenie wprowadzając nową funkcjonalność instrumentu płatniczego. Co więcej, banki wprowadzają samoregulacje w zakresie odpowiedzialności za kradzież środków pieniężnych z użyciem zbliżeniowych kart płatniczych,



Wykres 18. Odpowiedź na pytanie: „Jakich informacji nie może żądać od Ciebie przedstawiciel banku?" w zależności od płci

natomiast nie wynika ona wprost z ustawy o usługach płatniczych[33].

Podczas opracowywania procedur banki powinny pamiętać, że bezpieczeństwo nie może być priorytetem w każdej sytuacji – poziom zabezpieczeń musi być adekwatny do zagrożeń. Zachwianie równowagi w tym obszarze może spowodować, że usługa stanie się z punktu widzenia klienta całkowicie nieefektywna np. silne uwierzytelnianie lub autoryzacja przy każdorazowej transakcji zbliżeniowej byłaby rozwiązaniem bardzo problematycznym.

Eksperci zwracali uwagę na kwestie dostarczania regulaminów do klienta z użyciem poczty elektronicznej. Najlepsza praktyka w takim przypadku, to wykorzystanie silnego szyfrowania. Może to jednak oznaczać, że klient nie będzie chciał z takich zabezpieczeń korzystać. Z tego względu pojawiają się kompromisy – np. zabezpieczenie dokumentów przesyłanych pocztą elektroniczną za pomocą numeru PESEL. To nie są dobre rozwiązania, chociaż na pewno lepsze niż brak jakichkolwiek zabezpieczeń. W rzeczywistości odpowiednie postępowanie powinno polegać na zabezpieczeniu dokumentu wrażliwego bezpiecznym hasłem (np. 16 znakowym i spełniającym kryteria bankowej polityki bezpieczeństwa), a następnie przesłaniu tak zabezpieczonego dokumentu mailem i dostarczeniu hasła klientowi za pomocą oddzielnego kanału komunikacyjnego (np. SMS, albo – najlepiej – komunikatem aplikacji mobilnej).

Istnieje problem na styku klient – bankowy zespół ds. bezpieczeństwa. W przypadku realnej potrzeby dotarcie do takiego zespołu jest dla klienta praktycznie niemożliwe. Innymi słowy – bankowi specjaliści od bezpieczeństwa są poza zasięgiem klientów. W efekcie, jeżeli klienci zauważają, że coś złego wydarzyło się na ich koncie lub zdają sobie sprawę ze swojej pomyłki, nie istnieje prokliencka procedura pozwalająca na szybkie zablokowanie realizacji przelewu w każdej formie. W bankach funkcjonują też swoiste martwe strefy, np. od piątku, godz. 16:00 do poniedziałku, godz. 12:00, które dodatkowo uniemożliwiają kontakt.

3.3. Ergonomia rozwiązań

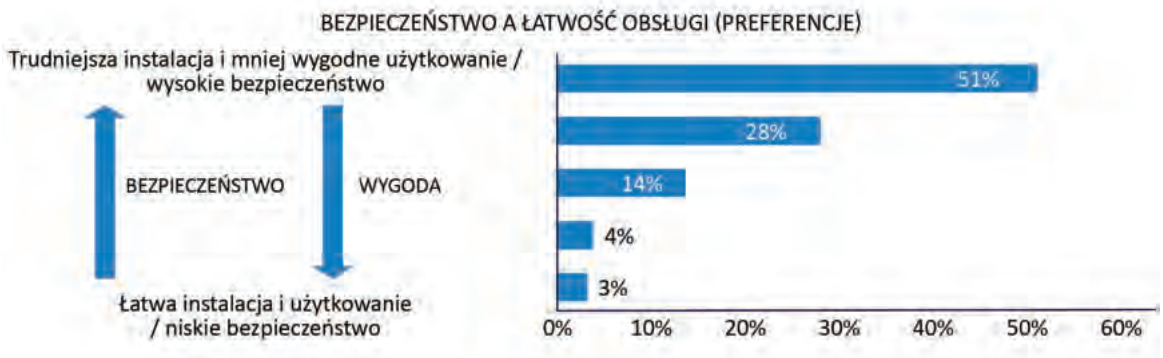
Istotną kwestią w czasie badania było ustalenie preferencji respondentów między bezpieczeństwem aplikacji bankowych, a łatwością ich użytkowania.

Kompromis, obejmujący spełnienie postulatu przyjazności aplikacji, jej łatwej i intuicyjnej obsługi, przy jednoczesnym zachowaniu rygorystycznych wymagań bezpieczeństwa jest wyznacznikiem, który znacząco wpływa na ostateczny kształt oprogramowania dla klientów i procedur związanych z jego obsługą. Szereg wymagań proceduralnych musi być wplecionych w taką formułę użytkowania aplikacji, która pozwoli na zachowanie najwyższego poziomu bezpieczeństwa z akceptowanym przez użytkownika końcowego poziomem skomplikowania instalacji i konfiguracji.

Badani eksperci wskazują na systematyczny rozwój rozwiązań z zachowaniem kompromisu pomiędzy ergonomią i bezpieczeństwem, przy czym sukcesu upatrują w ogólnych trendach środowiska i przyjętych kierunkach rozwoju. Na przestrzeni lat nowe rozwiązania stają się coraz łatwiejsze do wykorzystania, zaś w zakresie bezpieczeństwa korzystają z dopracowanych i wszechstronnie przetestowanych modułów odpornych na przełamanie zabezpieczeń.

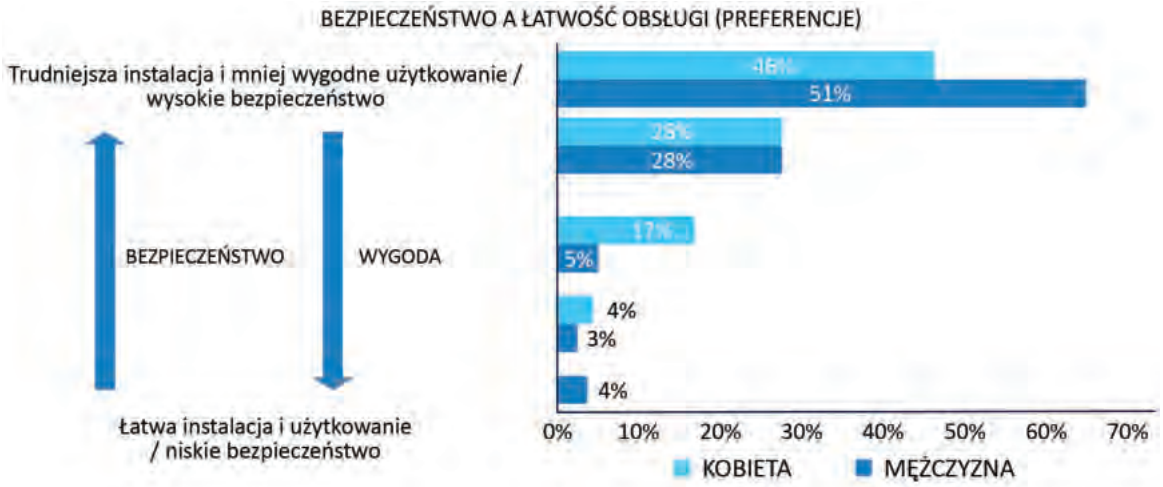
Przebadanie preferencji klientów bankowości elektronicznej w przedmiotowym zakresie pozwoliło zebrać wyniki przedstawione na wykresach 19 i 20.

Wykres 19 przedstawia preferencje klientów bankowości elektronicznej bez podziału na płeć. Widzimy, co należy uznać za pocieszające, że większość



Wykres 19. Rozkład preferencji odnośnie bezpieczeństwa a wygody obsługi aplikacji bankowych

[33] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz.U. 2011 nr 199 poz. 1175.



Wykres 20. Rozkład preferencji odnośnie bezpieczeństwa a wygody obsługi aplikacji bankowych w podziale na płeć

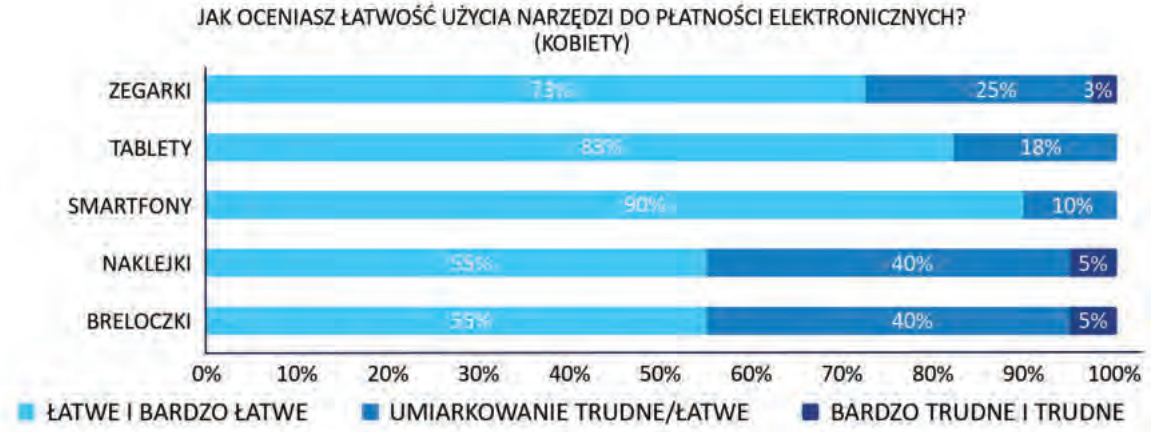
użytkowników skłania się ku bezpieczeństwu aplikacji, co oznacza trudniejszą instalację i mniej wygodne użytkowanie w miarę, jak wzrasta poziom bezpieczeństwa. Innymi słowy dla bezpieczeństwa aplikacji użytkownicy są w stanie w bardzo dużym stopniu zrezygnować z wygody, czyli łatwości instalacji i użytkowania, które niosłyby za sobą niskie bezpieczeństwo. W miarę, jak przesuwamy się od łatwej instalacji i użytkowania przy niskim bezpieczeństwie – odpowiednio 3% i 4% odpowiedzi respondentów – w kierunku trudniejszej instalacji i mniej wygodnego użytkowania przy wysokim bezpieczeństwie, udział procentowy odpowiedzi respondentów stopniowo wzrasta od 14% (co można uznać za oczekiwanie umiarkowanego bezpieczeństwa aplikacji przy umiarkowanie trudnej instalacji i użytkowaniu), przez 28%, aż do 51% (co oznacza wysokie bezpieczeństwo przy trudniejszej instalacji i mniej wygodnym użytkowaniu). Ten trend można uznać za zadowalający.

Uzupełnieniem wykresu 19 może być wykres 20, który dodatkowo wprowadza podział ze względu na płeć. Generalny trend związany z preferowaniem bezpieczeństwa ponad wygodą pozostaje – oczywiście – zachowany. Ciekawą obserwacją jest natomiast fakt, że występują pewne różnice na poziomie umiarkowanego bezpieczeństwa i umiarkowanej wygody, gdzie aż 17% mężczyzn i tylko 5% kobiet wyraziło takie oczekiwanie. Różnica na tym poziomie ma wpływ na wynik dotyczący wysokiego bezpieczeństwa przy trudniejszej instalacji i mniej wygodnym użytkowaniu – tutaj aż 65% kobiet i znacznie mniej, bo 46% mężczyzn, wyraża taką preferencję.

Reasumując, respondenci jednoznacznie wskazują na prymat bezpieczeństwa, przy czym to kobiety godzą się częściej na poniesienie dodatkowych nakładów na podniesienie bezpieczeństwa kosztem łatwości instalacji i użytkowania.

Należy zauważyć, że paleta urządzeń mobilnych, za pomocą których możliwe jest realizowanie płatności elektronicznych, jest coraz szersza. Również oferta banków w zakresie produktów i usług dostępnych za pomocą mobilnych kanałów komunikacyjnych, systematycznie się poszerza. Głównymi zaś wyznacznikami, które determinują chęć skorzystania z nowych rozwiązań, są prostota użytkowania i zaufanie. Wykresy 21 i 22 przedstawiają ocenę łatwości użycia wybranych narzędzi do płatności elektronicznych w rozbiciu na płeć, a wykres 23 dotyczy łatwości użycia produktów do płatności elektronicznych.

Na wykresie 21 zobrazowano procentowy udział odpowiedzi na pytanie „jak oceniasz łatwość użycia narzędzi do płatności elektronicznych?" w grupie kobiet. Za najłatwiejsze w obsłudze („łatwe i bardzo łatwe") kobiety uznały smartfony – tak odpowiedziało aż 90% kobiet, a tylko 10% z nich uznało, że są one „umiarkowanie trudne/łatwe" w obsłudze. Drugi w kolejności wynik uzyskały tablety, które przez 83% kobiet zostały określone jako „łatwe i bardzo łatwe" w obsłudze, a przez 18% respondentek zostały wskazane jako „umiarkowanie trudne/łatwe". Trzeci wynik to zegarki, które cieszą się w grupie kobiet bardzo dużym uznaniem, jeżeli chodzi o łatwość użycia, ponieważ wskazało je 73% respondentek. Jednocześnie już 25% kobiet odbiera zegarki jako „umiarkowanie trudne/łatwe" w użyciu. Pojawia się także ocena, którą można uznać za krytyczną, gdyż 3% respondentek określiło zegarki jako „bardzo trudne i trudne" w użyciu. Naklejki i breloczki cieszą się w grupie kobiet znacznie mniejszym uznaniem, jeżeli chodzi o łatwość użycia, co może wydawać się zadziwiające – odpowiednio 55% kobiet wskazało, że breloczki i naklejki są „łatwe i bardzo łatwe" w użyciu, aż 40%, że są „umiarkowanie trudne/łatwe" w użyciu i 5% określiło je jako „bardzo trudne i trudne".



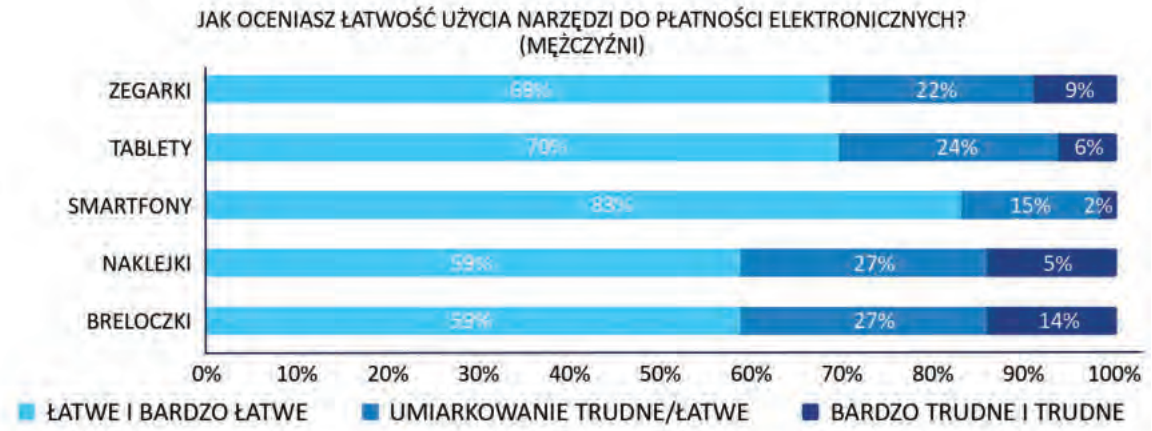
Wykres 21. Ocena łatwości użycia narzędzi do płatności elektronicznych w grupie kobiet

Wykres 22 przedstawia odpowiedzi na pytanie „Jak oceniasz łatwość użycia narzędzi do płatności elektronicznych?" w grupie mężczyzn. Jeżeli chodzi o ogólną percepcję łatwości użycia, to w przypadku kobiet i mężczyzn jest ona bardzo zbliżona. Przodują smartfony, a za nimi plasują się tablety i zegarki. Wartości procentowe udzielonych odpowiedzi są jednak niższe w obszarze „łatwe i bardzo łatwe" – odpowiednio 83% mężczyzn wskazało tutaj smartfony; 70% wskazało tablety i 69% wskazało zegarki. Z kolei 15% mężczyzn uznało smartfony za „umiarkowanie trudne/łatwe", a 2% określiło je jako „bardzo trudne i trudne" w użyciu. Sceptycyzm mężczyzn odnośnie łatwości użycia wzrasta w odniesieniu do tabletów i zegarków: 24% mężczyzn określiło tablety jako „umiarkowanie trudne/łatwe", a 6% określiło je jako „bardzo trudne i trudne" w użyciu; 22% mężczyzn odpowiedziało, że zegarki są „umiarkowanie trudne/łatwe" w użyciu, a 9% wybrało odpowiedź „bardzo trudne i trudne".

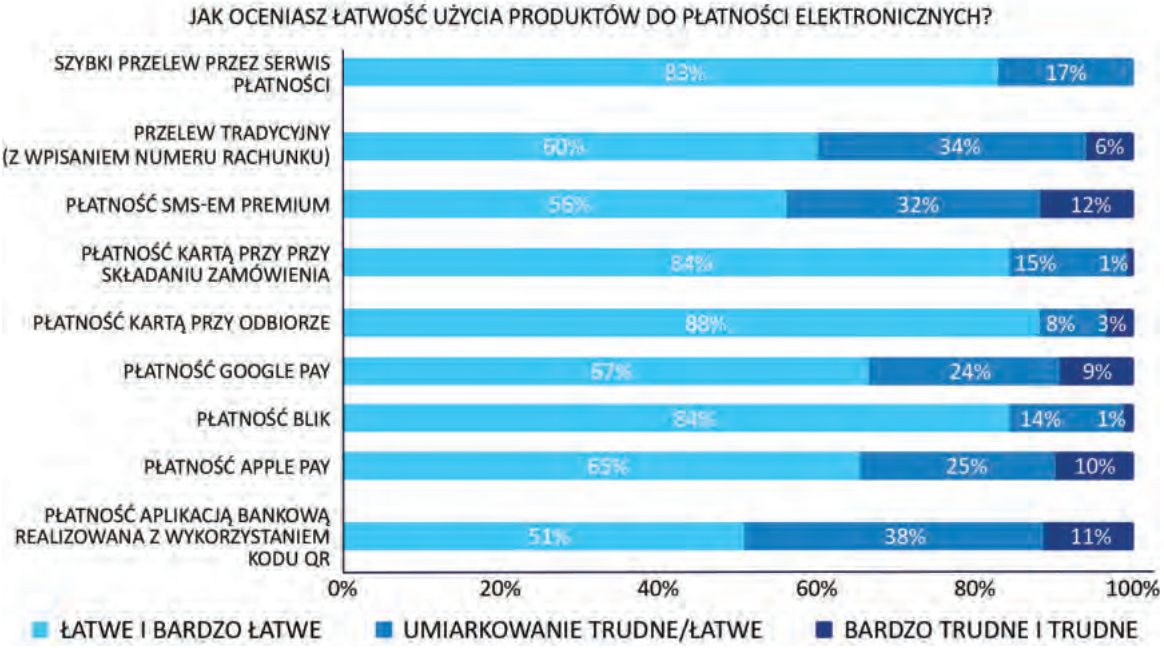
Skąd przeświadczenie, że naklejki i breloczki są trudniejsze w użyciu od np. smartfonów, które jest wyraźne zarówno w grupie kobiet, jak i mężczyzn? Wydaje się, że przedstawione wyniki mogą mieć związek z faktem, iż płatności realizowane za pomocą naklejek lub breloczków nie są powszechnie spotykane w Polsce – budzą więc podejrzliwość, co może przekładać się także na obniżoną percepcję w zakresie łatwości użycia.

Eksperci byli zgodni co do faktu, iż rozwiązania obecnie dostępne na rynku, czyli aplikacje lub płatności smartwatchami, są bardzo ergonomiczne. Podkreślano jednak obawę, że w niektórych przypadkach ergonomia może iść za daleko – tutaj jeden z rozmówców przedstawił następujący scenariusz: jeżeli jednorazowo wpiszemy kod PIN na smartwatchu i będzie on aktywny przez długi czas, to istnieje ryzyko, że ktoś, kto zbliży się do nas, teoretycznie może w ten sposób zatwierdzić transakcję. Pomimo, że jest to bardzo niskie ryzyko, to należy je odnotować.

Ciekawa sytuacja wyłania się w odniesieniu do produktów dla płatności elektronicznych (patrz wykres 23). O ile prym wiedzie tutaj tradycyjna karta płatnicza



Wykres 22. Ocena łatwości użycia narzędzi do płatności elektronicznych w grupie mężczyzn



Wykres 23. Ocena łatwości użycia produktów do płatności elektronicznych

(„płatność kartą przy odbiorze" jako „łatwą i bardzo łatwą" wskazało 88% respondentów, a „płatność kartą przy składaniu zamówienia" jako „łatwą i bardzo łatwą" wskazało 84% respondentów), to na kolejnym miejscu znajduje się BLIK (84% respondentów określiło go jako „łatwy i bardzo łatwy" w użyciu), przez co został potraktowany prawie na równi z szybkim przelewem przez serwis płatności lub płatnościami z użyciem karty. Warto podkreślić, że 3% respondentów określiło płatność kartą przy odbiorze jako „bardzo trudną i trudną" w użyciu. Dla płatności BLIK i płatności kartą przy składaniu zamówienia zrejestrowano 1% odpowiedzi „bardzo trudne i trudne", a rozpiętość odpowiedzi „umiarkowanie trudne i łatwe" dla czterech najpopularniejszych produktów do płatności elektronicznych jest następująca: 8% – płatność kartą przy odbiorze; 14% – płatność BLIK; 15% – płatność kartą przy składaniu zamówienia; 17% – szybki przelew przez serwis płatności.

Ciekawym jest także uznanie, jakim cieszą się płatności Google Pay i Apple Pay, co w zestawieniu z deklaracjami odnośnie wykorzystywanego urządzenia mobilnego przez respondentów (83% wskazuje, iż korzysta ze smartfonu – patrz wykres 24) nie powinno budzić wątpliwości, jeżeli chodzi o chęci wykorzystania tego typu rozwiązań przez klientów bankowości elektronicznej. Odpowiedzi kształtują się tutaj w sposób następujący (patrz wykres 23): 67% respondentów uważa, że Google Pay jest „łatwe i bardzo łatwe" w użyciu, a 65% wskazuje tutaj Apple Pay; 24% respondentów uważa Google Pay za „umiarkowanie trudne/łatwe" w użyciu, a 25% respondentów uważa Apple Pay za „umiarkowanie trudne/łatwe" w użyciu; z kolei 9% respondentów uznało Google Pay za „bardzo trudne i trudne" w użyciu, a 10% respondentów w taki sposób ocenia Apple Pay.

Najmniejszą popularnością cieszą się kolejno: przelew tradycyjny (z wpisaniem numeru rachunku" – 60% respondentów uważa go za „łatwy i bardzo łatwy", 34% respondentów określa go jako „umiarkowanie trudny/łatwy", a 6% respondentów wybrało odpowiedź „bardzo trudny i trudny"; płatność SMS-em premium – 56% respondentów uważa, że jest to „łatwa i bardzo łatwa" opcja, 32% respondentów wskazało odpowiedź „umiarkowanie trudne/łatwe", a 12% pytanych odpowiedziało, że tą opcję ocenia jako „bardzo trudną i trudną"; płatność aplikacją bankową realizowana z wykorzystaniem kodu QR – 51% respondentów wybrało tutaj odpowiedź „łatwe i bardzo łatwe", 38% respondentów odpowiedziało, że opcja ta jest „umiarkowanie trudna/łatwa", a 11% respondentów określiła ten produkt do płatności elektronicznych jako „bardzo trudny i trudny" w użyciu.

Eksperci podkreślali w zakresie ergonomii rozwiązań fakt, że komfort korzystania z dobrodziejstw bankowości elektronicznej (zdalnej) od samego początku jej istnienia wiąże się z pewnym ryzykiem. Kiedyś klient musiał inicjować transakcje osobiście, udając się w tym celu do placówki bankowej. Bankowość elektroniczna sprawiła, że klient może zainicjować transakcję w sposób zdalny, a skoro tak, to istnieje ryzyko, że taką samą operację może w jego imieniu wykonać także osoba trzecia, która wykorzysta

nieświadomość lub podatności klienta (ofiary). Istnieje więc ścisły związek ergonomii rozwiązań z obszarem bezpieczeństwa bankowości elektronicznej, co otwiera pole manewru dla przestępców stosujących socjotechnikę lub wykorzystujących podatności rozwiązań technicznych.

Podczas rozmów eksperci podkreślali też zalety biometrii, która pozwala na połączenie wygody użytkowania z bezpieczeństwem.

Trzeba wreszcie pamiętać, że są klienci świadomi ryzyka i tacy, którzy stawiają wyłącznie na wygodę. Świadomi użytkownicy potrafią kontaktować się z bankiem i np. wymuszać silne uwierzytelnienie przy każdej płatności – nawet za cenę wygody. Większość użytkowników ceni jednak szybkość i wygodę transakcji, szczególnie, jeżeli mają świadomość, że ta odbywa się na ryzyko dostawcy usługi płatniczej. Należy pamiętać, że jeżeli użytkownik chce płacić łatwo i przyjemnie, może mieć ograniczoną świadomość ryzyka związanego z obszarem bezpieczeństwa – np. może podpiąć swoją kartę płatniczą pod cudze urządzenie i silnie uwierzytelnić taką operację lub może pozwolić na przejęcie kontroli nad swoim urządzeniem osobom trzecim poprzez instalację oprogramowania do zdalnego zarządzania itd. Wszystko w imię szybkości i wygody.

W odniesieniu do ergonomii podkreślano potencjał elektronicznych portfeli (portmonetek), czyli usług Google Pay i Apple Pay (patrz wykres 23), które dodatkowo oferują wysoki poziom bezpieczeństwa. Wydaje się, że te rozwiązania mają potencjał, aby w przyszłości zyskać jeszcze większą popularność (patrz wykres 26 i 27).

3.4. Zmiany technologiczne

W ocenie ekspertów w ramach bankowości elektronicznej brak jest unikatowych i dedykowanych tylko tej sferze rozwiązań sprzętowych. Eksperci wskazują, że wprowadzane i wykorzystywane rozwiązania cechują się dużym poziomem dojrzałości technologicznej, tym niemniej zdarzają się sytuacje, gdy presja rynku i wynikający z konkurencji pośpiech powoduje wdrożenia, w których nie zawsze udaje się w sposób proceduralny zabezpieczyć pełne bezpieczeństwo klienta bankowości elektronicznej, co przejawiać się może w kłopotach z rozwiązaniem spornych sytuacji, gdy dane rozwiązanie wykorzystywane jest przez grupy przestępcze do działań na szkodę klienta banku.

W odniesieniu zaś do rozwiązań programowych (systemy, aplikacje) eksperci wskazują na uwagę, jaka przywiązywana jest do tworzenia bezpiecznych rozwiązań, w tym w szczególności testowania rozwiązań włącznie z niezależnymi testami bezpieczeństwa i organizowanymi konkursami typu „bug bounty".

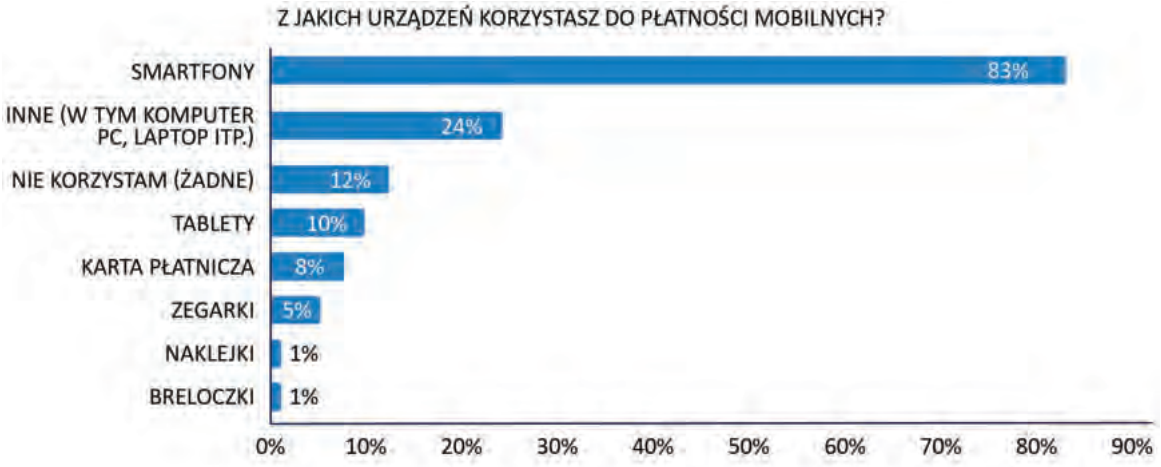
Z informacji, jakie można uzyskać od instytucji Rzecznika Finansowego wynika, iż nieustannie motywem wprowadzonych bądź planowanych zmian w zakresie sposobu zlecania i przeprowadzania transakcji jest szybkość i łatwość dostępu do usług bankowości elektronicznej. Podyktowane jest to komercyjną chęcią zatrzymania dotychczasowego klienta i pozyskania nowych klientów zachęcanych usługami świadczonymi w sposób nowoczesny i łatwy w obsłudze. Wysoki poziom bezpieczeństwa zapewniony jest przez monitoring funkcjonujący w czasie rzeczywistym w trybie detekcji i prewencji, co pozwala na uruchamianie automatycznych mechanizmów bezpieczeństwa. Takie podejście podyktowane jest z jednej strony odpowiedzialnością wobec klienta wynikającą z wdrożonej dyrektywy PSD2, jak i respektowania zasady, wedle której bezpieczeństwo to chęć uzyskania wiedzy, jak być o krok przed przestępcami.

W przypadku badanej grupy klientów bankowości elektronicznej jednym z podstawowych pytań, na jakie należało znaleźć odpowiedź, było, jaki jest poziom i zakres wykorzystywanych urządzeń do płatności elektronicznych. Z badań wynika jednoznacznie, iż smartfon jest narzędziem podstawowym (patrz wykres 24). Stał się on uniwersalnym narzędziem, które dzięki fenomenalnemu rozwojowi pozwala na wykorzystanie go jako substytutu komputera, tabletu i wielu innych urządzeń.

Na drugim miejscu respondenci wskazali, że do płatności mobilnych stosują urządzenia „Inne (w tym komputer PC, laptop itp.)" – taką odpowiedź wybrało 24% osób. Wynik ten jest stosunkowo ciekawy o tyle, że sugeruje, iż wielu klientów bankowości elektronicznej nie rozdziela ściśle bankowości internetowej, w której komputer PC lub laptop mają uzasadnienie, od bankowości mobilnej opartej przede wszystkim o smartfony. Z wykresu 25 możemy dowiedzieć się, że komputer był wskazywany przede wszystkim przez grupy wiekowe od 41 do 60 lat (6,7% respondentów) i od 26 do 40 lat (6,1% respondentów).

Wracając do wykresu 24 – zaskakująca w odpowiedzi jest deklaracja 12% badanych, iż nie korzystają z żadnych urządzeń do płatności mobilnych.

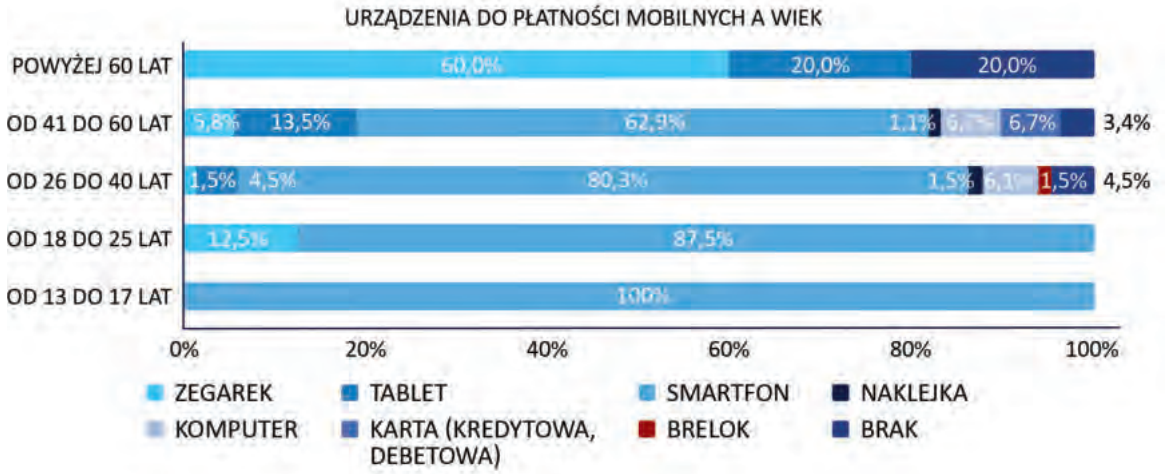
Znacznie lepsze zrozumienie preferencji klientów bankowości elektronicznej w obszarze urządzeń mobilnych przynosi analiza wykresu 25. Zegarki, stanowiące swoiste novum na rynku, przeważają u młodszych badanych (odpowiednio: 12,5% odpowiedzi w grupie wiekowej od 18 do 25 lat; 5,6% w grupie wiekowej od 41 do



Wykres 24. Wykorzystywane urządzenia mobilne do płatności mobilnych

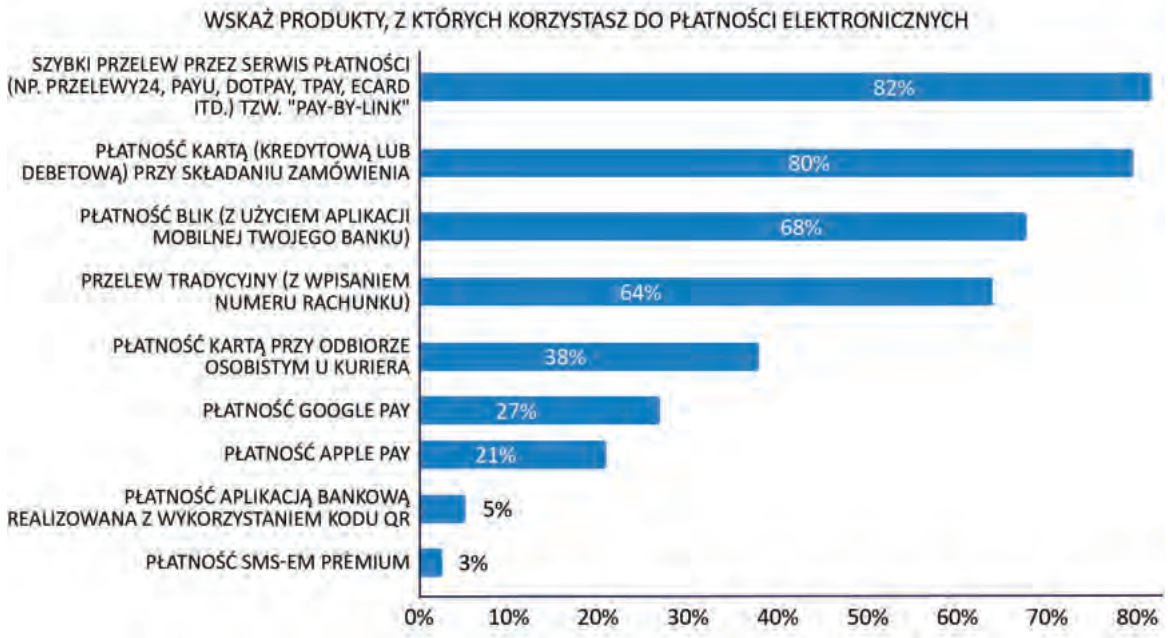
60 lat; 1,5% w grupie wiekowej od 26 do 40 lat). Tablety zaś pojawiają się u dojrzałych respondentów – odpowiednio: 4,5% w grupie wiekowej od 26 do 40 lat; 13,5% w grupie wiekowej od 41 do 60 lat; 20% w grupie wiekowej powyżej 60 lat. Smartfon został wybrany przez 100% respondentów z grupy wiekowej 13 do 17 lat. W grupie wiekowej od 41 do 60 lat 6,7% odpowiadających wskazało kartę (kredytową, debetową), a 1,1% naklejkę. Z kolei w grupie wiekowej od 26 do 40 lat 1,5% odpowiedzi oddano na naklejkę i na brelok.

Brak wykorzystania urządzeń do płatności mobilnych zadeklarowało aż 20% respondentów w grupie wiekowej powyżej 60 lat, 4,5% respondentów w grupie wiekowej od 26 do 40 lat i 3,4% respondentów w grupie wiekowej od 41 do 60 lat. Na podstawie posiadanych informacji trudno uzasadnić taką odpowiedź, ale możliwe, że respondenci mieli zamiar w ten sposób podkreślić, iż nie wykorzystują np. smartfonów podczas płatności. Kwestia ta może stanowić przyczynek dalszych, pogłębionych badań.



Wykres 25. Wiek a wykorzystywane urządzenia mobilne do płatności mobilnych

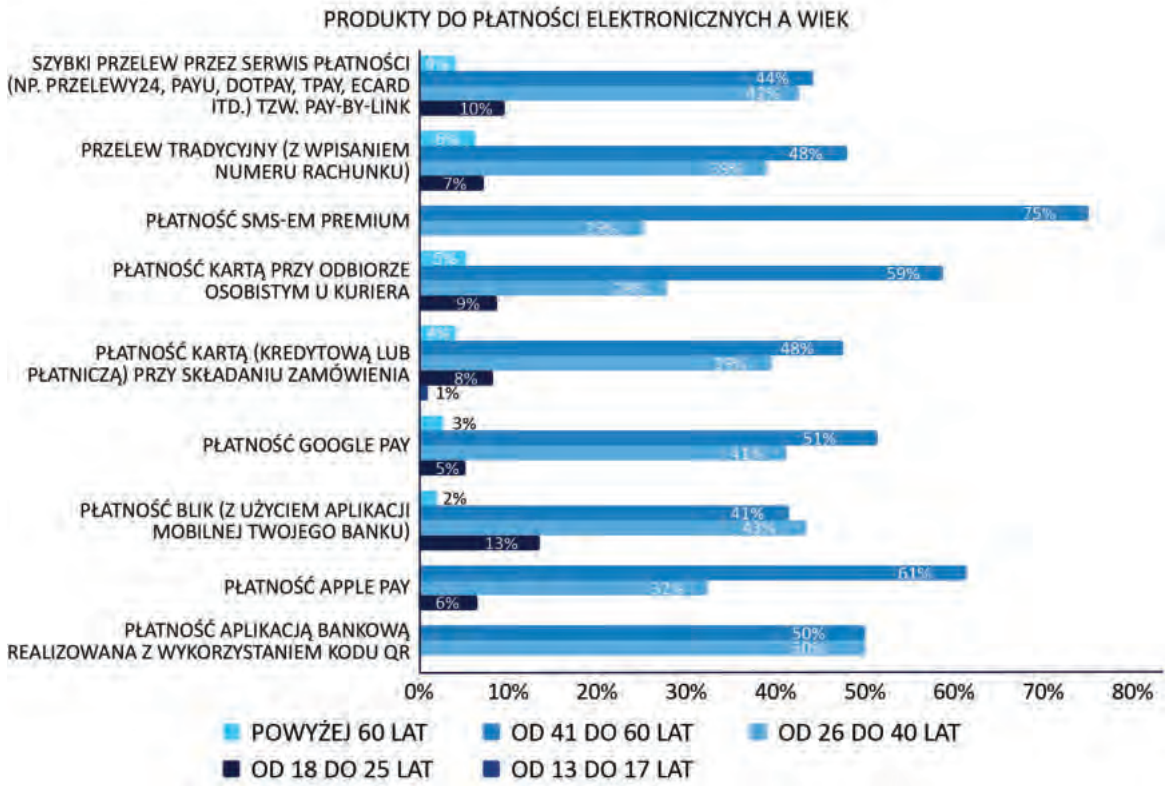
Na wykresie 26 przedstawiono preferencje klientów w zakresie produktów wykorzystywanych do płatności elektronicznych. Największą popularnością cieszą się tutaj szybkie przelewy przez serwis płatności (np. Przelewy24, PayU, Dotpay, tPay, eCard itd.) tzw. „Pay-by-Link", które wskazało 82% respondentów oraz płatności kartą (kredytową lub debetową) przy składaniu zamówienia, które wskazało 80% respondentów. Mniejszą popularnością cieszą się płatności BLIK, które wybrało 68% respondentów oraz przelewy tradycyjne (z wpisaniem numeru rachunku), które wybrało 64% respondentów. Płatność kartą przy odbiorze osobistym u kuriera wskazało 38% respondentów. Na dalszych miejscach są odpowiednio płatności Google Pay (27% respondentów), płatności Apple Pay (21% respondentów), a najmniej rozpowszechnione wśród klientów są płatności aplikacją bankową realizowane z wykorzystaniem kodu



Wykres 26. Popularność produktów wykorzystywanych do płatności elektronicznych wśród respondentów

QR (5% respondentów) i płatności SMS-em premium (3% respondentów).

Wykres 27 obrazuje preferencje klientów w zakresie produktów wykorzystywanych do płatności elektronicznych w podziale na grupy wiekowe i stanowi uszczegółowienie wyników przedstawionych na wykresie 26. Płatności elektroniczne są powszechnie wykorzystywane przede wszystkim przez grupy wiekowe od 41 do 60 lat i od 26 do 40 lat, przy czym preferencje są tutaj istotnie zróżnicowane w przypadku produktów, takich jak: płatność SMS-em premium (produkt



Wykres 27. Popularność produktów wykorzystywanych do płatności elektronicznych wśród respondentów w poszczególnych grupach wiekowych

wskazało 75% respondentów w grupie wiekowej od 41 do 60 lat i tylko 25% respondentów w grupie wiekowej od 26 do 40 lat), płatność kartą przy odbiorze osobistym u kuriera (produkt wskazało 59% respondentów w grupie wiekowej od 41 do 60 lat i 28% respondentów w grupie wiekowej od 26 do 40 lat) oraz płatność Apple Pay (produkt wskazało 61% respondentów w grupie wiekowej od 41 do 60 lat i 32% respondentów w grupie wiekowej od 26 do 40 lat). Wspomniane produkty są więc wyraźnie częściej używane przez respondentów w grupie wiekowej od 41 do 60 lat. Co ciekawe, o ile widoczna jest tutaj wyraźna różnica w odniesieniu do Apple Pay, to w przypadku podobnego produktu Google Pay jest ona już znacznie mniejsza, ponieważ produkt ten wskazało 51% respondentów w grupie wiekowej od 41 do 60 lat i 41% respondentów w grupie wiekowej od 26 do 40 lat.

Kolejną interesującą obserwacją jest fakt, że zarówno w grupie wiekowej od 41 do 60 lat, jak i w grupie wiekowej od 26 do 40 lat identyczną popularnością cieszą się płatności aplikacją bankową realizowane z wykorzystaniem kodu QR. Respondenci z obydwu grup wskazywali ten produkt w 50% przypadków.

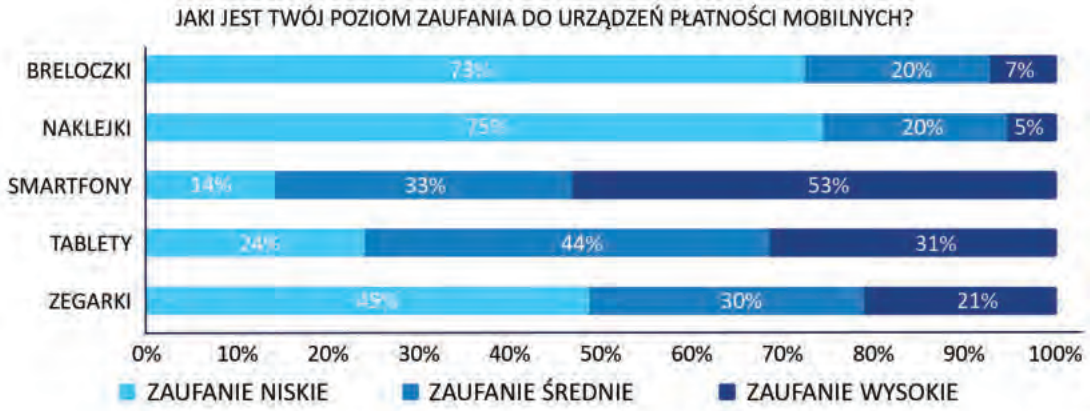
Pozostałe grupy wiekowe są reprezentowane w dużo mniejszym stopniu dla poszczególnych produktów do płatności elektronicznych, przy czym grupy wiekowe powyżej 60 lat, od 18 do 25 lat i od 13 do 17 lat w ogóle nie wskazywały takich produktów, jak: płatność SMS -em premium i płatność aplikacją bankową realizowana z wykorzystaniem kodu QR. Grupa od 13 do 17 lat – reprezentowana w najmniejszym stopniu – wskazała wyłącznie płatność kartą (kredytową lub debetową) przy składaniu zamówienia, co stanowiło tylko 1% wszystkich odpowiedzi dla tego typu produktu.

Wykres 28 przedstawia poziom zaufania klientów do urządzeń płatności mobilnych. Najmniejszym zaufaniem cieszą się naklejki i breloczki – odpowiednio: 75% i 73% respondentów określiła swoje zaufanie jako niskie w stosunku do tych urządzeń. Na trzecim miejscu, jeżeli chodzi o niskie zaufanie respondentów, są zegarki – obserwujemy tutaj 49% odpowiedzi „zaufanie niskie", 30% odpowiedzi „zaufanie średnie" i 21% odpowiedzi „zaufanie wysokie". Można więc przyjąć, że zegarki jako urządzenia płatności mobilnych wciąż traktowane są ze sporą rezerwą ze strony klientów.

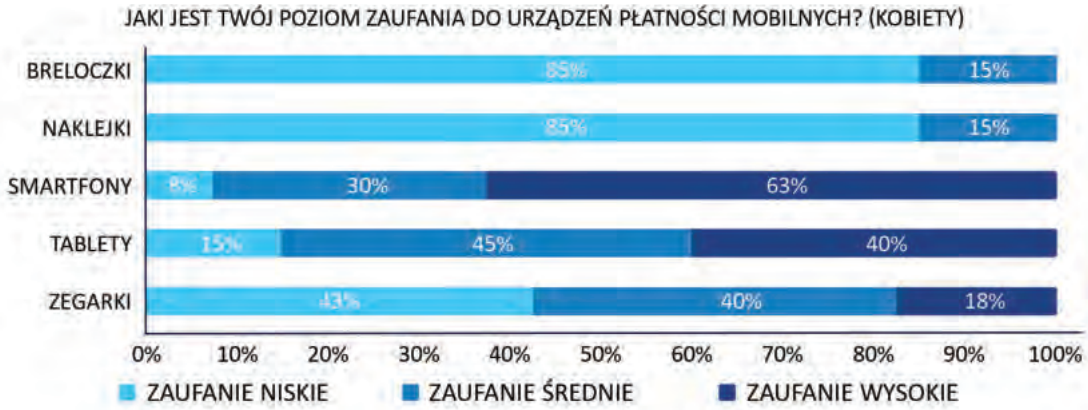
Z kolei największym zaufaniem respondenci darzą smartfony (53% odpowiedzi „zaufanie wysokie" i 33% odpowiedzi „zaufanie średnie") oraz tablety (31% odpowiedzi „zaufanie wysokie" i 44% odpowiedzi „zaufanie średnie"). Warto przypomnieć, że smartfony są najczęściej wykorzystywanym urządzeniem do płatności mobilnych (patrz wykres 24) i wskazane były przez 83% respondentów, przy czym tablety wybrało tylko 10% respondentów.

Dokładniejsze zrozumienie, w jaki sposób kształtuje się poziom zaufania do urządzeń płatności mobilnych wśród klientów, dają wykresy 29 i 30 – odpowiednio przedstawiają one rozkład odpowiedzi w grupie kobiet i mężczyzn. Porównując odpowiedzi kobiet i mężczyzn dostrzegamy, że w grupie kobiet naklejki i breloczki cieszą się dużo niższym zaufaniem (85% odpowiedzi „zaufanie niskie" dla obydwu urządzeń) niż w grupie mężczyzn (odpowiednio 71% i 68% odpowiedzi „zaufanie niskie" dla obydwu urządzeń). W przypadku zegarków, kobiety wyrażają większe zaufanie (18% odpowiedzi „zaufanie wysokie", 40% odpowiedzi „zaufanie średnie" i 43% odpowiedzi „zaufanie niskie") niż mężczyźni (22% odpowiedzi „zaufanie wysokie", 26% odpowiedzi „zaufanie średnie" i 52% odpowiedzi „zaufanie niskie").

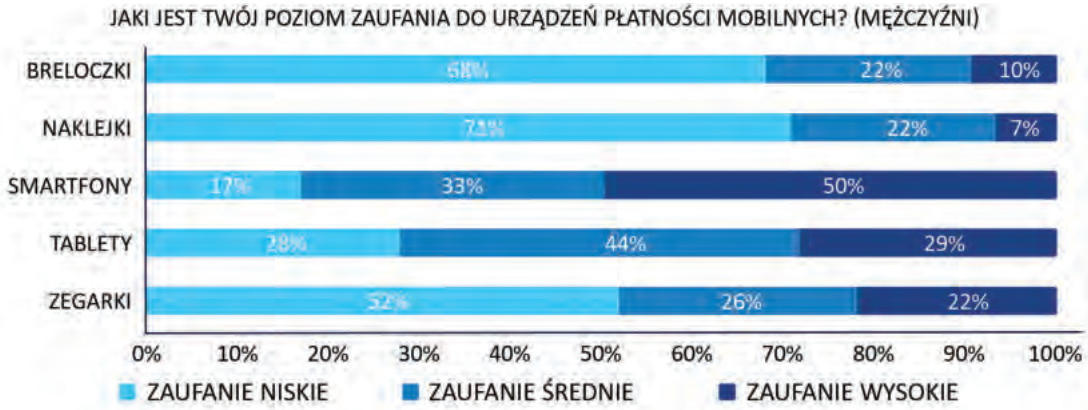
W obydwu grupach najwyższym zaufaniem cieszą się smartfony – przy czym kobiety ufają im nieco bardziej (63% odpowiedzi „zaufanie wysokie", 30% odpowiedzi „zaufanie średnie" i tylko 8% odpowiedzi „zaufanie niskie") niż mężczyźni (50% odpowiedzi



Wykres 28. Poziom zaufania respondentów do urządzeń płatności mobilnych (kobiety i mężczyźni)



Wykres 29. Poziom zaufania respondentów do urządzeń płatności mobilnych (kobiety)



Wykres 30. Poziom zaufania respondentów do urządzeń płatności mobilnych (mężczyźni)

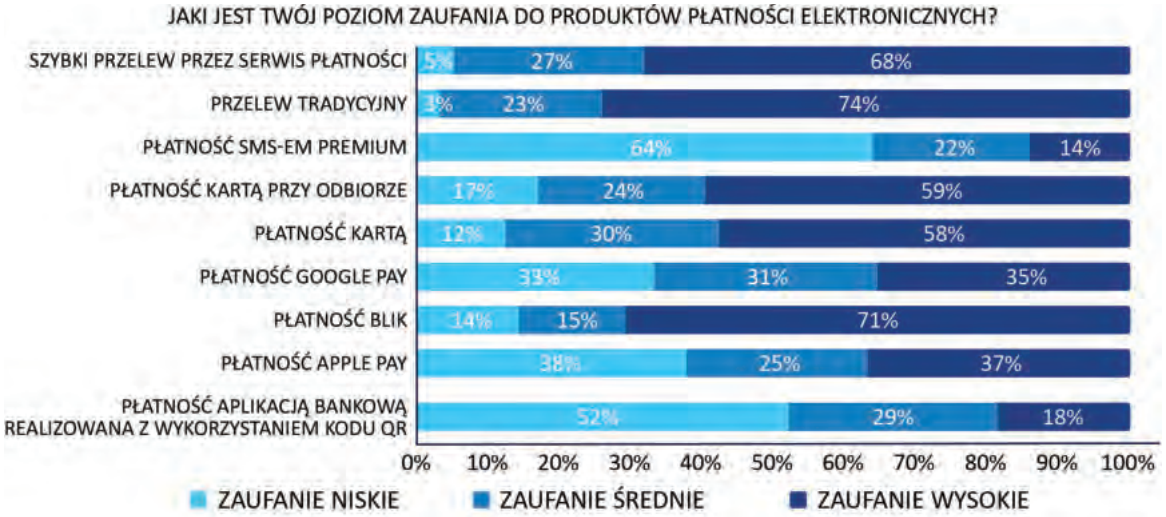
„zaufanie wysokie", 33% odpowiedzi „zaufanie średnie" i aż 17% odpowiedzi „zaufanie niskie"). Tablety są z kolei darzone istotnie większym zaufaniem przez kobiety (40% odpowiedzi „zaufanie wysokie", 45% odpowiedzi „zaufanie średnie" i 15% odpowiedzi „zaufanie niskie") niż przez mężczyzn (29% odpowiedzi „zaufanie wysokie", 44% odpowiedzi „zaufanie średnie" i aż 28% odpowiedzi „zaufanie niskie").

Reasumując, można przyjąć, że kobiety są bardziej sceptyczne od mężczyzn w stosunku do nowinek (breloczki i naklejki), jeżeli chodzi o poziom zaufania, ale są skłonne darzyć wyraźnie większym zaufaniem urządzenia znajdujące się w powszechnym użyciu (smartfony i tablety).

Dotychczasowe rozważania warto uzupełnić pomiarem poziomu zaufania do produktów płatności elektronicznych (patrz wykres 31). Największym zaufaniem respondentów cieszą się: przelew tradycyjny (74% odpowiedzi „zaufanie wysokie", 23% odpowiedzi „zaufanie średnie" i tylko 3% odpowiedzi „zaufanie niskie"); szybki przelew przez serwis płatności (68% odpowiedzi „zaufanie wysokie", 27% odpowiedzi „zaufanie średnie" i tylko 5% odpowiedzi „zaufanie niskie"); a wreszcie płatność BLIK, chociaż pojawia się już tutaj znaczący element braku zaufania (71% odpowiedzi „zaufanie wysokie", 15% odpowiedzi „zaufanie średnie" i aż 14% odpowiedzi „zaufanie niskie").

Następnie w kolejności rankingu zaufania produktów płatności elektronicznych plasuje się płatność kartą (kredytową lub debetową), która darzona jest wysokim zaufaniem przez 58% respondentów, średnim zaufaniem przez 30% respondentów i niskim zaufaniem przez 12% respondentów. Zbliżony poziom zaufania klienci wyrazili w stosunku do płatności kartą przy odbiorze (59% odpowiedzi „zaufanie wysokie", 24% odpowiedzi „zaufanie średnie" i 17% odpowiedzi „zaufanie niskie").

Ciekawym jest porównanie zaufania do płatności elektronicznych realizowanych za pomocą Apple Pay (37% odpowiedzi „zaufanie wysokie", 25% odpowiedzi „zaufanie średnie" i 38% odpowiedzi „zaufanie niskie") i Google Pay (35% odpowiedzi „zaufanie wysokie", 31% odpowiedzi „zaufanie średnie" i 33% odpowiedzi „zaufanie niskie"). Obydwa produkty darzone są przez klientów podobnym poziomem zaufania z lekką przewagą Google Pay.



Wykres 31. Poziom zaufania respondentów do produktów płatności mobilnych (kobiety i mężczyźni)

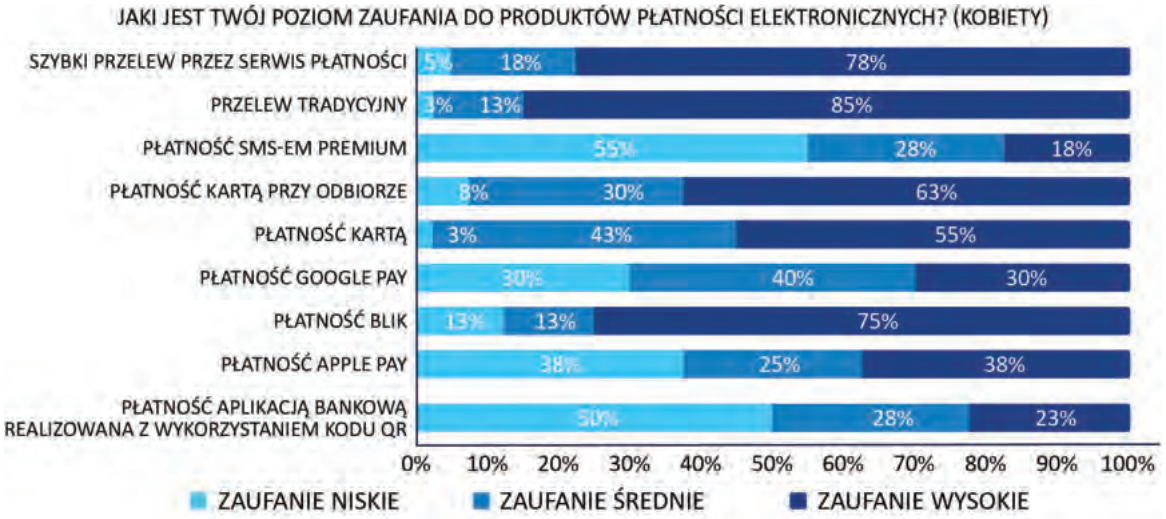
Zdaniem respondentów najmniej godnymi zaufania produktami płatności elektronicznych są płatność SMS-em premium (14% odpowiedzi „zaufanie wysokie", 22% odpowiedzi „zaufanie średnie" i aż 64% odpowiedzi „zaufanie niskie") oraz płatność aplikacją bankową z wykorzystaniem kodu QR (18% odpowiedzi „zaufanie wysokie", 29% odpowiedzi „zaufanie średnie" i aż 52% odpowiedzi „zaufanie niskie").

Wykresy 32 i 33 przedstawiają bardziej szczegółowy obraz kształtowania się poziomu zaufania do produktów płatności elektronicznych, który uwzględnia płeć – odpowiednio zobrazowane są odpowiedzi kobiet i mężczyzn.

W obydwu grupach do najbardziej zaufanych produktów płatności elektronicznych zaliczyć można: przelew tradycyjny, szybki przelew przez serwis płatności i płatność BLIK. Odpowiada to danym ogólnym, przedstawionym na wykresie 31, przy czym kobiety darzą wspomniane produkty nieco wyższym zaufaniem.

W przypadku przelewu tradycyjnego aż 85% kobiet wybrało odpowiedź „zaufanie wysokie", 13% wybrało odpowiedź „zaufanie średnie" i tylko 3% wybrało odpowiedź „zaufanie niskie". Odpowiedzi mężczyzn rozłożyły się następująco: 71% odpowiedzi „zaufanie wysokie", 26% odpowiedzi „zaufanie średnie" i tylko 4% odpowiedzi „zaufanie niskie" – widoczny jest więc nieco mniejszy entuzjazm, jeżeli chodzi o poziom zaufania do tego produktu.

Z kolei szybki przelew przez serwis płatności jest oceniany następująco: kobiety (78% odpowiedzi „zaufanie wysokie", 18% odpowiedzi „zaufanie średnie" i tylko 5% odpowiedzi „zaufanie niskie"), mężczyźni (65% odpowiedzi „zaufanie wysokie", 29% odpowiedzi



Wykres 32. Poziom zaufania respondentów do produktów płatności mobilnych (kobiety)

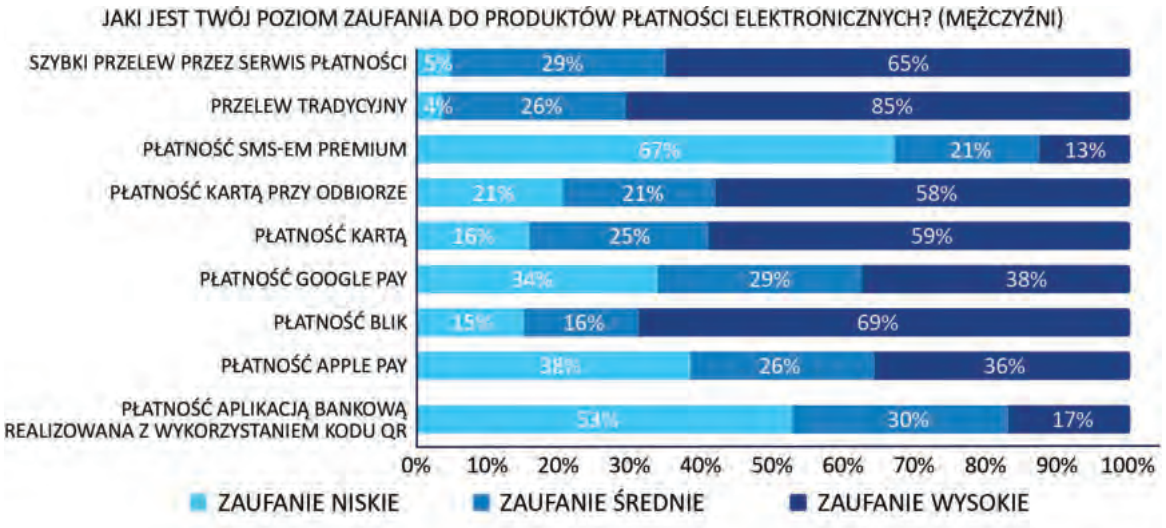
„zaufanie średnie” i tylko 5% odpowiedzi „zaufanie niskie”). W przypadku tego produktu mężczyźni wyrażają już istotnie mniejszy poziom zaufania.

Mężczyźni darzą płatność BLIK nieco mniejszym poziomem zaufania niż kobiety – respondenci w tej grupie wskazali 69% odpowiedzi „zaufanie wysokie”, 16% odpowiedzi „zaufanie średnie” i 15% odpowiedzi „zaufanie niskie”. W grupie kobiet odpowiedzi ukształtowały się następująco: 75% odpowiedzi „zaufanie wysokie”, 13% odpowiedzi „zaufanie średnie” i 13% odpowiedzi „zaufanie niskie”.

W przypadku następnych pod względem poziomu zaufania produktów płatności elektronicznych, czyli płatności kartą (kredytową lub debetową) i płatności kartą przy odbiorze, ma zastosowanie ta sama reguła: mężczyźni są mniej ufni od kobiet. Płatność kartą (kredytową lub debetową) została oceniona przez kobiety następująco: 55% odpowiedzi „zaufanie wysokie”, 43% odpowiedzi „zaufanie średnie” i tylko 3% odpowiedzi „zaufanie niskie”. Mężczyźni z kolei odpowiadali z wyraźnie większą ostrożnością: 59% odpowiedzi „zaufanie wysokie”, 25% odpowiedzi „zaufanie średnie” i aż 16% odpowiedzi „zaufanie niskie”. Rozkład odpowiedzi dla płatności kartą przy odbiorze w grupie kobiet wygląda tak: 63% odpowiedzi „zaufanie wysokie”, 30% odpowiedzi „zaufanie średnie” i 8% odpowiedzi „zaufanie niskie”. Dla grupy mężczyzn: 58% odpowiedzi „zaufanie wysokie”, 21% odpowiedzi „zaufanie średnie” i aż 21% odpowiedzi „zaufanie niskie”. Różnice w poziome zaufania są więc znaczące.

Płatności Google Pay wygrywają z Apple Pay, jeżeli chodzi o poziom zaufania w obydwu grupach. W przypadku Apple Pay poziom deklarowanego zaufania kobiet (38% odpowiedzi „zaufanie wysokie”, 25% odpowiedzi „zaufanie średnie” i 38% odpowiedzi „zaufanie niskie”) jest porównywalny do tego, który zadeklarowali mężczyźni (36% odpowiedzi „zaufanie wysokie”, 26% odpowiedzi „zaufanie średnie” i 38% odpowiedzi „zaufanie niskie”). Natomiast w odniesieniu do Google Pay zauważalne są znaczące różnice. Kobiety udzieliły tutaj następujących odpowiedzi: 30% respondentek wskazało odpowiedź „zaufanie wysokie”, 40% respondentek wskazało odpowiedź „zaufanie średnie” i 30% respondentek wskazało odpowiedź „zaufanie niskie”. Rozkład odpowiedzi w grupie mężczyzn wygląda następująco: 38% odpowiedzi „zaufanie wysokie”, 29% odpowiedzi „zaufanie średnie” i 34% odpowiedzi „zaufanie niskie”. Mężczyźni są więc odrobinę mniej ufni od kobiet wobec produktu Google Pay.

Produkty takie jak płatność SMS-em premium i płatność aplikacją bankową z wykorzystaniem kodu QR cieszą się najmniejszym zaufaniem zarówno w grupie kobiet, jak i mężczyzn. Jeżeli chodzi o płatność SMS-em premium, to niskie zaufanie widoczne jest wyraźniej w przypadku mężczyzn – odpowiadali oni w następujący sposób: tylko 13% odpowiedzi „zaufanie wysokie”, 21% odpowiedzi „zaufanie średnie” i aż 67% odpowiedzi „zaufanie niskie”. Kobiety odpowiadały tutaj nieco mniej sceptycznie: 18% odpowiedzi „zaufanie wysokie”, 28% odpowiedzi „zaufanie średnie” i 55% odpowiedzi „zaufanie niskie”. Dla płatności aplikacją bankową z wykorzystaniem kodu QR różnice między grupą kobiet i mężczyzn są bardziej subtelne: 17% respondentów wybrało odpowiedź „zaufanie wysokie”, 30% respondentów wybrało odpowiedź „zaufanie średnie” i 53% respondentów wybrało odpowiedź „zaufanie niskie” w grupie mężczyzn; 23% respondentek wskazało tutaj odpowiedź „zaufanie wysokie”, 28% respondentek wskazało odpowiedź „zaufanie średnie” i 50% respondentek wskazało odpowiedź „zaufanie niskie”.



Wykres 33. Poziom zaufania respondentów do produktów płatności mobilnych (mężczyźni)

Eksperci, wskazując biometrię, zwracali uwagę na fakt, że zmiany technologiczne mogą mieć korzystny wpływ na bezpieczeństwo klienta bankowości elektronicznej i jednocześnie oferować wysoki komfort użycia. Przy czym istotna jest tutaj zaawansowana biometria – np. można przyjąć, że rozpoznawanie twarzy na platformie Apple iOS jest dużo bardziej skuteczne niż w przypadku platformy Google Android, na której powinno używać się odcisków palca. Zwrócono uwagę, że dane biometryczne muszą być przechowywane bezpośrednio na urządzeniu i nie mogą być eksportowane na zewnątrz.

W kontekście kompromisu między wygodą a bezpieczeństwem, warto zwrócić uwagę na możliwość podpięcia aplikacji przechowującej i generującej jednorazowe kody. Część ekspertów wyraźnie podkreślała zalety rozwiązania polegającego na wykorzystaniu zewnętrznej aplikacji uwierzytelniającej, takiej jak Google Authenticator lub Microsoft Authenticator – w idealnym scenariuszu najlepiej, aby aplikacja uwierzytelniająca działała na osobnym urządzeniu, pozwalając użytkownikowi potwierdzić transakcję realizowaną na innym urządzeniu. Oczywiście potwierdzenie może zostać dokonane także na tym samym urządzeniu, ale wówczas – co należy wziąć pod uwagę – cała operacja jest mniej bezpieczna. Przykładowy scenariusz może wyglądać następująco: klient wykonuje transakcję na tablecie, ale uwierzytelnia ją na smartfonie lub odwrotnie, albo, jeżeli dysponuje dwoma smartfonami, może skonfigurować rozwiązanie tak, aby na jednym urządzeniu wykonywać transakcje, a na drugim je potwierdzać. Kluczowe jest tutaj założenie, że rozdzielenie funkcji pomiędzy urządzeniami sprawia, iż ewentualny atak będzie dużo trudniejszy do przeprowadzenia.

W rozmowach podkreślano również, że zmiany technologiczne mogą wprowadzać nowe ryzyka – tutaj przykładem może być łatwość zapłacenia skradzioną klientowi zbliżeniową kartą płatniczą do kwoty 100 PLN przed jej zastrzeżeniem. Z kolei, jeżeli karta płatnicza została powiązana ze smartfonem, to w przypadku kradzieży urządzenia sprawca – zanim zapłaci kartą płatniczą ofiary – musi odblokować ekran. Jeżeli ekran jest zablokowany za pomocą kodu PIN lub odcisku palca, to środki finansowe właściciela urządzenia są bezpieczniejsze. Utrata smartfonu nie będzie więc automatycznie oznaczała możliwości płacenia zbliżeniowo, tak jak w przypadku zwykłej karty zbliżeniowej.

Istnieją więc tutaj pewne nieporozumienia i możliwe komplikacje. W powszechnym rozumieniu zakłada się, że zmiany technologiczne będą przekładały się na większe bezpieczeństwo bankowości elektronicznej, podczas gdy klient mimo wszystko oczekuje wygody. Ponadto zmiany technologiczne mogą być wymuszane wymaganiami regulacyjnymi, co nie musi oznaczać troski o wygodę użycia danego rozwiązania. Można przyjąć, że zmiany technologiczne mają korzystny wpływ na bezpieczeństwo klienta bankowości elektronicznej, jeżeli wprowadzane funkcje i mechanizmy są ergonomiczne i są jak najbardziej przejrzyste dla użytkownika – nie wymuszają na nim dodatkowych działań. Jeżeli bowiem na użytkowniku wymuszane są dodatkowe działania, to ten najczęściej będzie starał się ich unikać i nie będzie z nich korzystał.

Wreszcie, jeżeli mówimy o ewolucyjnym rozwoju technologii i w tym sensie rozumiemy wpływ zmian technologicznych na bezpieczeństwo, to na pewno będzie on korzystny, podczas gdy naprawdę innowacyjne technologie, swoiste rewolucje, zawsze będą wprowadzać nowe, nierozpoznane ryzyka. Można więc przyjąć, że na bezpieczeństwo klienta bankowości elektronicznej wpływają przede wszystkim: ewolucyjne zmiany technologiczne, większa transparentność, większa łatwość użytkowania (ergonomia), jak najmniej elementów wymagających uczenia się od klienta-użytkownika i odpowiednia komunikacja dotycząca zasadności oraz celowości wprowadzania zmian.

Należy także podkreślić rolę zarządzania ryzykiem technologicznym. Każda technologia ma jakieś podatności, dlatego ocena ryzyka winna być przeprowadzana regularnie, okresowo, a w przypadku zidentyfikowania nowych ryzyk, należy opracowywać akcje mitygacyjne (mityganty). Usunięcie zidentyfikowanych podatności danej technologii wymaga czasu m. in. dlatego, że bank nie jest jej wytwórcą, a to ma istotny wpływ na szybkość opracowania i wdrożenia poprawek. Mając na uwadze korzystny wpływ zmian technologicznych na bezpieczeństwo klientów, ważne jest więc, aby w procesie wdrażania nowej technologii obok biznesu, będącego najczęściej sponsorem projektu i technologii – strony realizującej projekt, od samego początku uczestniczyli przedstawiciele działu bezpieczeństwa – jest to zresztą zgodne z wymogami Rekomendacji D KNF[34].

[34] Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf, stan z dn. 8 sierpnia 2021.

ROZDZIAŁ IV

PROGRAM ANALITYCZNO BADAWCZY

Kierunki rozwoju usług dla klienta bankowości elektronicznej

Niniejszy rozdział ma charakter prognostyczny i stanowi próbę wskazania kierunków dalszego rozwoju bankowości elektronicznej. Jednym z kolejnych etapów ewolucji bankowości jest przejście od – charakterystycznej dla bankowości elektronicznej – dystrybucji wielokanałowej do dystrybucji omnikanałowej i realizacja koncepcji klientocentryczności, co stanowi fundament transformacji cyfrowej banków i ma prowadzić do powstania bankowości cyfrowej. Coraz częściej wskazuje się też na fakt ścisłego powiązania usług bankowych z nowoczesnymi technologiami.

Jednocześnie należy mieć świadomość, że transformacji cyfrowej ulega obszar przestępczości bankowej. Nowoczesne technologie, które znajdują się w obszarze zainteresowania banków, pozostają także do dyspozycji przestępców – niosą więc nie tylko korzyści, ale także ryzyko, które należy uwzględniać podczas podejmowania decyzji strategicznych dotyczących włączenia danego rozwiązania do bankowego portfolio techniczno-technologicznego.

Informacje przedstawione w poszczególnych podrozdziałach są wynikiem:

- analizy artykułów naukowych i literatury specjalistycznej dotyczącej omawianego zagadnienia,
- badań terenowych/ankietowych klientów bankowości elektronicznej w celu określenia ich poziomu świadomości i umiejętności korzystania z bankowości elektronicznej,
- wywiadów eksperckich przeprowadzanych z respondentami, którzy reprezentowali środowisko związane z sektorem bankowym, działami bezpieczeństwa i IT instytucji finansowych oraz z biegłymi sądowymi.

4.1. Nowe usługi

Rynek usług w zakresie bankowości elektronicznej ewoluuje wraz z rozwojem środowiska techniczno-technologicznego, które tworzy otaczającą nas rzeczywistość. Nowe rozwiązania w zakresie komunikacji, możliwości identyfikacji klienta usług bankowych, szybkość i łatwość w komunikacji podmiotów sektora bankowości prowadzi do nieustającego rozwoju formy i zakresu usług, jakie mogą być świadczone dla klientów bankowości. W tym podrozdziale na podstawie badań wskazane zostały usługi, które będą wdrażane w celu usprawnienia i ułatwienia funkcjonowania środowiska klienta bankowości elektronicznej.

Obok smartfonów, które wpłynęły na rozwój bankowości elektronicznej w odmianie mobilnej, należy podkreślić potencjał urządzeń ubieralnych i typu smart, które są jedną z sił napędowych transformacji cyfrowej. Tego typu rozwiązania są bowiem w stanie nie tylko tworzyć nowe kanały komunikacji z klientami, a więc sprzyjają omnikanałowości, lecz także dostarczają dużej ilości danych na temat klientów, co w połączeniu z technologiami z obszaru Big Data (związanymi z przetwarzaniem wielkich zbiorów danych) wychodzi naprzeciw postulatowi klientocentryczności bankowości cyfrowej. Dotykamy tutaj problematyki profilowania klientów.

Banki, które potrafią wykorzystać wielkie zbiory danych, wliczając w to dane transakcyjne, informacje z mediów społecznościowych, najróżniejsze formy korespondencji z klientami, mogą uzyskiwać dużo większą wiedzę na temat działań i preferencji klientów niż kiedykolwiek wcześniej i budować na tej wiedzy przewagę konkurencyjną[35]. Profilowanie pozwala więc osiągać korzyści finansowe – i to nie tylko w zakresie dopasowywania bieżącej oferty do konkretnego klienta, w preferowanym przez niego kanale komunikacji, ale także poprzez przewidywanie jego przyszłych zachowań czy optymalizację ryzyka. Bank posiada mnóstwo użytecznych informacji na temat danego klienta dotyczących nie tylko jego majątku, lecz także tego, czy terminowo płaci za usługi, w jakich sklepach i co kupuje (wyciągi z kart kredytowych). Dane te mogą być łączone z informacjami ze źródeł zewnętrznych, np. portali społecznościowych i firm telekomunikacyjnych[36], co z kolei pozwoli lepiej ocenić np. ryzyko kredytowe związane z danym klientem lub nawet wybraną ich grupą.

Najważniejszym osiągnięciem ostatnich lat są kryptowaluty, z których największą popularność uzyskał bitcoin (BTC), chociaż warto zwrócić uwagę także na ether, litheon, ripple i inne. Kryptowaluty stanowią instrument bardzo szeroko wykorzystywany przez uczestników rynków finansowych i indywidualnych inwestorów. Jednocześnie postrzega się je często jako pieniądz przyszłości z uwagi na takie ich zalety, jak (rzekomy) brak presji inflacyjnej (typowej dla fiducjarnych jednostek pieniężnych, emitowanych przez współczesne banki centralne), wygoda i szybkość obsługi czy przejrzystość oraz bezpieczeństwo transakcji tymi jednostkami. Można je zatem postrzegać jako sposób na reformę i zwiększenie stabilności współczesnych systemów pieniężnych. Z drugiej strony, kryptowaluty wywołują też liczne kontrowersje, dotyczące przede wszystkim ich prawnego statusu, trudnego do zrozumienia dla przeciętnego odbiorcy

[35] Raport Big Data w bankowości, https://www.zbp.pl/getmedia/eb647392-2e7f-48fd-8bbd-4803d0d84dec/Raport_BD_1411_final, ZBP, stan z dn. 8 sierpnia 2021, s. 4.
[36] W. Kurowski, *Mafia 2.0. Jak organizacje przestępcze kreują wartość w erze cyfrowej, Poltext, Warszawa 2015, s. 227.*

procesu ich kreacji i transferu (bazujących na zastosowaniu kryptografii) czy wreszcie bardzo częstych fluktuacji wartości[37].

Rozwiązaniem godnym szczególnego wyróżnienia jest system płatności BLIK. Zdaniem niektórych ekspertów jest to dobre i bezpieczne rozwiązanie, ale brakuje jakby świadomości, o co w tym rozwiązaniu chodzi, skoro wciąż rejestruje się dużą liczbę oszustw związanych z użyciem BLIK-a.

Sugerowany kierunek rozwoju, który wychodziłby naprzeciw postulatom klientocentryczności i omnikanałowości, wiąże się z powstaniem zintegrowanych platform typu „elektroniczne okienko bankowe". Podstawowe założenie dla tego typu rozwiązań jest takie, że powinny one pokrywać w kanałach elektronicznej komunikacji ofertę banków w sposób całościowy. Co jednak kluczowe, muszą one pozwalać na taki poziom silnego uwierzytelniania i autoryzacji, który nie pozwoli na późniejsze podważenie faktu dokonania jakiejś operacji.

Podkreślić należy znaczenie powiązań pomiędzy usługami płatniczymi, dzięki którym możliwe będzie płynne i automatyczne przekierowanie klienta za pośrednictwem zaufanego kanału z jednego serwisu do drugiego. Podstawowym założeniem jest, aby tego typu operacja nie wymagała dodatkowego logowania przy przekierowaniu, np. w momencie, kiedy klient zamierza dokonać przelewu. Osiągnięcie takiego stanu rzeczy możliwe będzie przy wykorzystaniu federalizacji usług i federalizacji zarządzania tożsamością, dzięki którym klient uzyska możliwość wykonania różnych działań – nie tylko działań w swojej usłudze bankowej, lecz także w innych, potrzebnych mu usługach. Taki kierunek rozwoju wydaje się doskonale spełniać postulat klientocentryczności w zakresie dostępności usług „tu i teraz".

Można więc przyjąć, że właściwymi kierunkami rozwoju są: integracja i federalizacja usług. W tym kontekście należy jednak przywołać koncepcję *Zero Trust* („zero zaufania" lub „brak zaufania" – tł. własne). Oznacza ona, że nie należy ufać niczemu wewnątrz bądź na zewnątrz naszego otoczenia, a dodatkowo ograniczać sloty czasowe trwania transakcji, które nie powinny być otwarte zbyt długo. Tutaj potrzebne są rzeczywiste ograniczenia, ale także konieczne jest monitorowanie tego, co dzieje się w danej sesji. Jeżeli zaobserwujemy coś nietypowego, należy taką sesję natychmiast przerywać lub skłaniać klienta do ponownego uwierzytelnienia np. za pomocą komponentu biometrycznego – takie rozwiązania nie generują dodatkowych, wysokich kosztów, a istotnie podnoszą poziom bezpieczeństwa. Co więcej, jeżeli chodzi o biometrię, to ponowne żądanie użycia odcisku palca lub wskazanie twarzy nie stanowi dla klienta dużego obciążenia, co wychodzi naprzeciw oczekiwaniom związanym z komfortem wykorzystania bankowości elektronicznej. Sytuacja wyglądałaby tutaj z punktu widzenia komfortu użytkownika znacznie gorzej, gdyby musiał ponownie wprowadzać długie i skomplikowane kombinacje znakowe, spełniające kryteria przyjętej polityki bezpieczeństwa.

Istotną kwestią jest potrzeba włączania usług dodatkowych do oferty banku, co wynika nie tylko z chęci wyjścia naprzeciw oczekiwaniom klientów (klientocentryczność) i uzyskania przewagi rynkowej, lecz także z regulacji – kluczowa jest tutaj dyrektywa PSD2 (ang. *Payment Services Directive*)[38], która weszła w życie w dniu 13 stycznia 2016 r. Zmieniła ona dotychczasową działalność dostawców usług płatniczych, w szczególności banków, w kierunku modelu tzw. otwartej bankowości (ang. *Open Banking*).

W ciągu ostatnich kilku lat nastąpiły istotne zmiany w obszarze płatności detalicznych pod względem innowacji technologicznych. Doprowadziło to do wzrostu liczby płatności elektronicznych (w szczególności w odniesieniu do bankowości mobilnej) oraz pojawienia się na rynku nowych graczy. Do tej pory zasadniczo tylko klienci banków mieli bezpośredni dostęp do swoich rachunków płatniczych i możliwość zlecania transakcji płatniczych. Zgodnie z dyrektywą PSD2, filozofia dostępu do rachunków płatniczych zmieniła się znacząco, ponieważ uprawnione *podmioty trzecie* (ang. *Third Party Provider, TTP*) mogą w imieniu i za zgodą klienta uzyskać dostęp do informacji o rachunku lub zlecać realizację płatności[39]. Dzięki temu TPP są w stanie świadczyć usługi dodatkowe w kooperacji z bankiem. Do polskiego porządku prawnego dyrektywa PSD2 została wprowadzona przez nowelizację ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych[40].

Uzupełnieniem wymogów dyrektywy PSD2 jest *Rozporządzenie Delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę*

[37] P. Marszałek, Kryptowaluty – pojęcie, cechy, kontrowersje, Studia BAS, nr 1(57)/2019, s. 107.

[38] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015L2366&from=PL, stan z dn. 8 sierpnia 2021.

[39] K. Leżoń, *Otwarta bankowość w świetle wymogów dyrektywy PSD2 - wyzwania i perspektywy rozwoju dla polskiego sektora FinTech, KNF, Warszawa 2019, s. 16.*

[40] Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111991175, stan z dn. 8 sierpnia 2021.

Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji[41] (ang. *Regulatory and Technical Standards, RTS*). Jest to kluczowy akt prawny, mający istotne znaczenie dla osiągnięcia celów PSD2 dotyczących ochrony konsumentów, promowania innowacji i poprawy bezpieczeństwa usług płatniczych w całej Unii Europejskiej. Dokument określa wymogi w zakresie stosowania silnego uwierzytelniania klienta oraz zasady komunikacji dostawców prowadzących rachunki płatnicze (np. banków) z podmiotami świadczącymi usługi dostępu do rachunku (TTP)[42].

Integracja banków z TTP – w myśl idei otwartej bankowości i dyrektywy PSD2 – możliwa jest dzięki udostępnianiu API (ang. *Application Programming Interface* – interfejs programistyczny aplikacji). Istotnym kryterium jest tutaj standaryzacja tego typu interfejsów, warto więc wyróżnić projekt *PolishAPI* – polski standard, który definiuje interfejs na potrzeby usług świadczonych przez strony trzecie w oparciu o dostęp do rachunków płatniczych. Twórcy standardu zakładają jego stały rozwój w odpowiedzi na zmiany regulacyjne, technologiczne i biznesowe na rynku polskim oraz europejskim. Zmiany będą publikowane jako kolejne wersje specyfikacji standardu PolishAPI[43]. Uczestnikami projektu są Związek Banków Polskich wraz ze stowarzyszonymi bankami komercyjnymi i spółdzielczymi, Spółdzielcze Kasy Oszczędnościowo-Kredytowe, Polska Organizacja Niebankowych Instytucji Płatności wraz ze stowarzyszonymi firmami, Polska Izba Informatyki i Telekomunikacji, Polska Izba Ubezpieczeń, Krajowa Izba Rozliczeniowa, Biuro Informacji Kredytowej i Polski Standard Płatności[44].

4.2. Nowe rozwiązania

Wykres 34 przedstawia rozkład odpowiedzi na pytanie: „co sądzisz na temat płatności autoryzowanych za pomocą biometrii (np. tęczówką oka, liniami papilarnymi – odciskiem palca itp.?". Respondentów poproszono o udzielenie odpowiedzi

Wykres 34. Zainteresowanie respondentów płatnościami autoryzowanymi za pomocą biometrii

w postaci krótkiej wypowiedzi pisemnej (komentarza). W oparciu o analizę treści wypowiedzi ustalono, że większość, bo aż 56% respondentów, wyraziła poparcie dla tego typu rozwiązań (wypowiedź sklasyfikowana jako odpowiedź „tak"), a 18% gotowa jest tego typu rozwiązania rozważyć (wypowiedź sklasyfikowana jako odpowiedź „może"). Nieprzychylnie wypowiedziało się 26% respondentów – nie są oni zainteresowani rozwiązaniami w zakresie bezpieczeństwa bankowości elektronicznej, które bazowałyby na biometrii (wypowiedź sklasyfikowana jako „nie"). Uwidacznia się tutaj tendencja do ostrożnego przyswajania nowoczesnych rozwiązań w obszarze bezpieczeństwa bankowości elektronicznej. Większość komentarzy respondentów podkreślała wygodę użytkownika, wyższy poziom bezpieczeństwa i skuteczność rozwiązań biometrycznych podczas autoryzacji płatności.

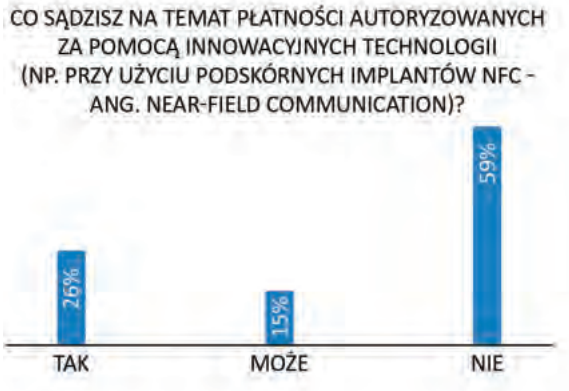
Na wykresie 35 zobrazowano odpowiedzi na pytanie dotyczące płatności autoryzowanych za pomocą innowacyjnych technologii, np. przy użyciu podskórnych implantów NFC (ang. *Near-Field Communication*). Respondentów poproszono tutaj o przedstawienie krótkiej wypowiedzi pisemnej (komentarza). W wyniku analizy treści wypowiedzi ustalono, że 59% z nich spełnia kryteria odpowiedzi „nie". Świadczy to o tym, że większość klientów nie jest zainteresowana innowacyjnymi rozwiązaniami opartymi o implanty NFC. Dla porównania, 26% respondentów wyraziła zainteresowanie (wypowiedzi sklasyfikowane jako odpowiedź „tak"), a 15% respondentów potencjalne zainteresowanie (wypowiedzi sklasyfikowane jako odpowiedź „może"). Większość komentarzy respondentów wyrażała obawy związane z bezpieczeństwem i za daleko idącym stopniem ingerencji w sferę intymną użytkownika. Tylko pojedyncze wypowiedzi podkreślały zalety tego typu rozwiązań lub zwracały uwagę, że są one nieuniknione (tutaj jednak trudno zgodę zrównywać z entuzjazmem).

[41] Rozporządzenie Delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0389&from=PL, stan z dn. 17 grudnia 2020.

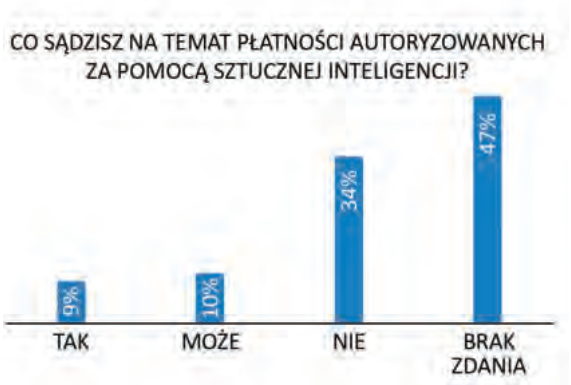
[42] K. Leżoń, *Otwarta bankowość w świetle wymogów dyrektywy PSD2 - wyzwania i perspektywy rozwoju dla polskiego sektora FinTech, KNF, Warszawa 2019, s. 19.*

[43] *O PolishAPI, https://polishapi.org/, stan z dn. 8 sierpnia 2021.*

[44] *O PolishAPI, https://polishapi.org/, stan z dn. 8 sierpnia 2021.*



Wykres 35. Zainteresowanie respondentów płatnościami autoryzowanymi za pomocą innowacyjnych technologii (np. przy użyciu podskórnych implantów NFC – ang. *Near -Field Communication*)



Wykres 36. Zainteresowanie respondentów płatnościami autoryzowanymi za pomocą sztucznej inteligencji

Odpowiedzi zestawione na wykresie 36 dotyczą pytania „co sądzisz na temat płatności autoryzowanych za pomocą sztucznej inteligencji?". Autorzy badania nie mieli tutaj na myśli żadnego konkretnego rozwiązania. Celem było poznanie intuicji klientów bankowości elektronicznej w odniesieniu do samej idei przeniesienia procesu autoryzacji na zewnątrz, co w rzeczywistości oznacza dla użytkownika utratę autonomii w zakresie podejmowania decyzji autoryzacyjnych. Wyniki badania są zadowalające. Respondenci odpowiadali na pytanie w postaci krótkiej wypowiedzi – komentarza. Z analizy udzielonych odpowiedzi wynika, że większość respondentów przychyla się do odpowiedzi „brak zdania", co prawdopodobnie spowodowane było mieszanką sceptycyzmu i brakiem bardziej sprecyzowanej wizji płatności autoryzowanych za pomocą sztucznej inteligencji – zarejestrowano tutaj 47% odpowiedzi. W drugiej kolejności pojawiły się odpowiedzi kategorycznie odrzucające tego typu pomysł – w toku analizy treści ustalono, że 34% wypowiedzi respondentów spełnia kryteria odpowiedzi „nie". Idea związana z zastosowaniem sztucznej inteligencji w procesie autoryzacji transakcji zyskała tylko 10% potencjalnych zwolenników (odpowiedź „może"). Całkowite poparcie wyraziło tutaj jedynie 9% respondentów. W większości przypadków respondenci zwracali uwagę w swoich wypowiedziach na zagrożenia związane z utratą autonomii na rzecz algorytmu sztucznej inteligencji lub zastanawiali się, w jaki dokładnie sposób tego typu rozwiązanie miałoby działać. Przeważały komentarze sceptyczne i podkreślające brak zaufania. Z kolei niektórzy eksperci, z którymi przeprowadzano wywiady na potrzeby niniejszego raportu, zwracali uwagę, że zastosowanie sztucznej inteligencji w obszarze autoryzacji otwiera całkiem nowy wymiar potencjalnych przestępstw socjotechnicznych: „na pracownika banku", „na policjanta" itp.

Eksperci zwracali uwagę, że wśród nowych rozwiązań w obszarze bankowości elektronicznej należy podkreślić przede wszystkim te, które oparte są na biometrii (np. silne uwierzytelnianie transakcji w sposób bezpieczny i wygodny z punktu widzenia klienta) oraz sztucznej inteligencji.

W pierwszym przypadku warto mieć na uwadze, że bardzo często będziemy mieć do czynienia z tzw. pseudobiometrią. Potwierdzenie transakcji z użyciem odcisku palca lub rozpoznawania twarzy to w rzeczywistości działanie w oparciu o uproszczony model biometryczny. Co do płatności potwierdzanych w ten sposób można więc przyjąć, że biometria lub pseudobiometria sprzyjają wygodzie, ale pojawia się aspekt ryzyka. Jeżeli faktycznie wykorzystywana ma być pełna biometria i od tego ma zależeć bezpieczeństwo środków finansowych klientów, to konieczne jest zachowanie szczególnej ostrożności. Brak bowiem dobrych narzędzi rozliczeniowych, dokumentujących to, co wydarzyło się aż do momentu autoryzacji transakcji. Co więcej, klient nie posiada np. dostępu do dziennika zdarzeń na koncie – pełne informacje są wyłącznie po stronie banku. W związku z tym powstaje kilka dylematów: w jaki sposób upewnić się, że autoryzacja biometryczna na pewno została zrealizowana przez konkretnego klienta? Należy mieć tutaj na uwadze ograniczenia współczesnych urządzeń biometrycznych (tzw. pseudobiometria), które w niektórych okolicznościach mogą być skutecznie oszukiwane przez przestępców. W takim razie, jak obsłużyć ewentualne reklamacje? Jakie atrybuty powinny być zachowywane podczas autoryzacji biometrycznej, aby później skutecznie przeprowadzić postępowanie reklamacyjne? Pytania te wciąż nie mają jednoznacznych odpowiedzi, dlatego też, pomimo że technologie biometryczne mają duży potencjał w zakresie bezpieczeństwa i wygody użycia, to rysuje się tutaj pewien margines związany z brakiem pełnego zaufania.

W drugim przypadku chodzi o oprogramowanie, które stosując algorytmy sztucznej inteligencji, jest w stanie wykrywać anomalie w zachowaniu płatnika będącego jednocześnie użytkownikiem platformy społecznościowej (np. Facebook) w celu ochrony jego środków finansowych (analiza behawioralna). Rozwiązanie takie, w przypadku wykrycia anomalii, może zablokować wykonanie podejrzanych działań np. transakcji. Jest też w stanie „uczyć się" zachowań typowych dla chronionego użytkownika. Należy jednak podkreślić, że w żadnym wypadku sztuczna inteligencja nie powinna być wykorzystywana w taki sposób, aby odbierać człowiekowi autonomię decyzji – ma wspierać ludzi, ale nie ich zastępować. Dodatkowym obszarem wykorzystania technologii z kręgu sztucznej inteligencji jest analiza wielkich zbiorów danych np. na potrzeby profilowania. Sztuczna inteligencja wciąż niesie za sobą ograniczenia nie tylko techniczne i prawne, lecz także etyczne, pomimo tego, że podkreśla się jej duży potencjał.

Istotne są również rozwiązania oparte o tokeny – np. generowane za pomocą aplikacji typu Google Authenticator lub Microsoft Authenticator, które mogą być instalowane na urządzeniach końcowych. Zaletą tych rozwiązań jest to, że w przyszłości powinny uniezależnić klientów od stałego atrybutu bezpieczeństwa (np. stałe, niezmieniane hasło), ponieważ unikalny token generowany jest automatycznie i regularnie.

ROZDZIAŁ V

PROGRAM ANALITYCZNO BADAWCZY

Nowe zagrożenia w środowisku cyberbezpieczeństwa i kierunki przeciwdziałania

Wykres 37 przedstawia odpowiedzi na pytanie „O których zagrożeniach zostałeś poinformowany lub masz świadomość ich występowania?". Badano tutaj świadomość klienta bankowości elektronicznej w odniesieniu do nowych zagrożeń w środowisku cyberbezpieczeństwa. Ogólna świadomość zagrożeń może być uznana za wysoką. Największa liczba respondentów potwierdziła, że została poinformowana przez bank lub ma świadomość istnienia zagrożenia związanego z fałszywym kontaktem od pracownika banku (91% respondentów odpowiedziało na to pytanie twierdząco, a tylko 9% przecząco). Na niższym, chociaż wciąż wysokim poziomie, uplasowały się takie zagrożenia, jak phishing i SPAM. W obydwu przypadkach 78% respondentów wybrało odpowiedź twierdzącą, a 22% odpowiedź przeczącą. Nieco mniej osób przyznało, że zostały poinformowane przez bank lub posiadają świadomość zagrożeń związanych z fałszywym kontaktem ze strony Policji celem zabezpieczenia konta bankowego – tutaj 72% respondentów wskazało odpowiedź twierdzącą, a 28% wskazało odpowiedź przeczącą. Najmniej osób przyznało się do posiadania wiedzy na temat zagrożeń związanych z fałszywym kontaktem od rachmistrza spisowego w ramach spisu powszechnego – odpowiednio 67% odpowiedzi twierdzących i 33% odpowiedzi przeczących.

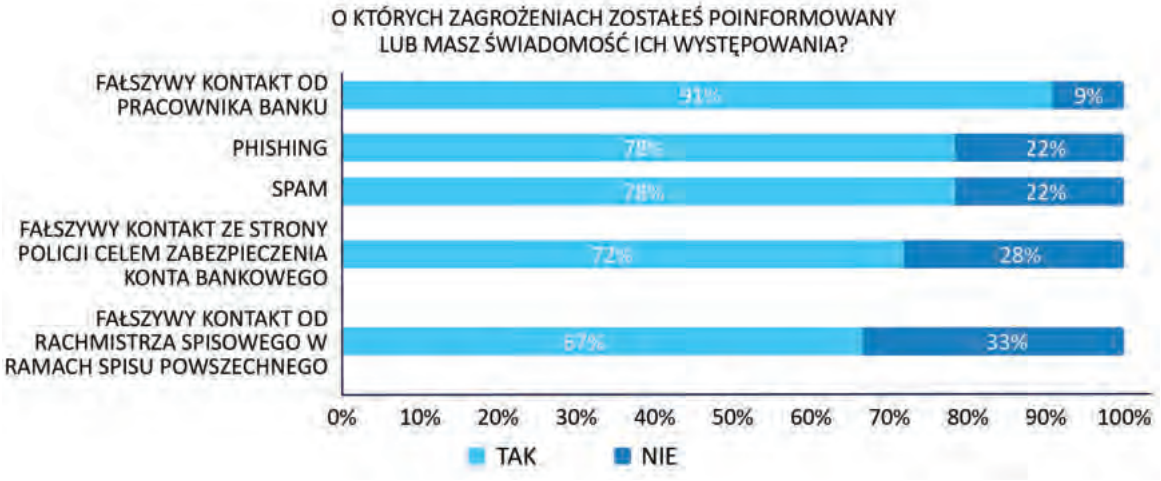
Warto zauważyć, że zagrożenia związane z fałszywym kontaktem są w rzeczywistości wariacją uniwersalnego scenariusza, w którym przestępca podszywa się pod dowolną osobę, działającą w określonym kontekście sprzyjającym uwiarygodnieniu podejmowanych czynności, celem zmuszenia ofiary do przekazania swoich środków finansowych – odpowiedzi związane z fałszywym kontaktem ze strony pracownika banku, policjanta czy rachmistrza spisowego można więc traktować jako jedną kategorię zagrożeń. Różnice w wynikach można utożsamiać do pewnego stopnia z rankingiem popularności poszczególnych wariantów tego samego przestępstwa – jest ich zresztą dużo więcej, a w przyszłości na pewno będą pojawiać się nowe pomysły. Przestępcy dostosowują bowiem uniwersalny scenariusz do potrzeb chwili i określonej kategorii ofiar.

Istotny wydaje się fakt, że chociaż aż 91% respondentów jest świadoma zagrożenia związanego z fałszywym kontaktem od pracownika banku, to – zdaniem ekspertów – właśnie przestępstwa oparte na podszywaniu się pod pracowników banku biją dziś rekordy popularności i okazują się skuteczne. Obecnie jest to jeden z najpopularniejszych wektorów ataków, można więc przyjąć, że istnieje duża podatność po stronie klientów w tym zakresie. Dodatkową kwestią, którą warto poruszyć w kontekście otrzymanych wyników, jest pytanie o faktyczny poziom zaawansowania socjotechniki przestępczej.

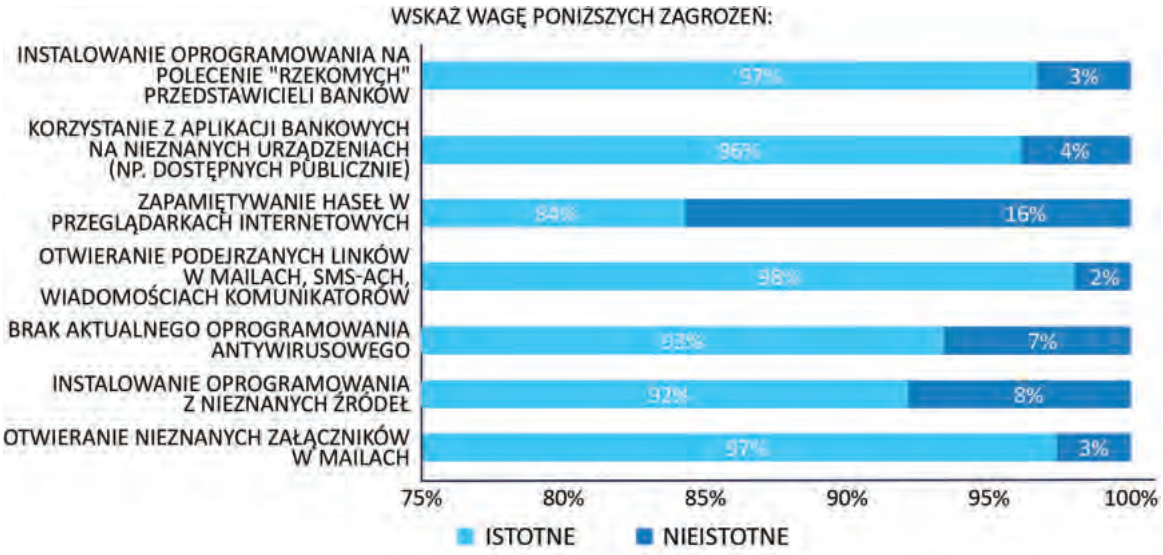
Obserwacja stanu faktycznego, jeżeli chodzi o częstotliwość i rodzaj incydentów związanych z środowiskiem bezpieczeństwa klientów bankowości elektronicznej, skłaniała ekspertów do postawienia wniosku, iż wysoki poziom świadomości zagrożeń nie niesie za sobą realnej odporności.

Przyjmując grupowanie, w którym za istotne przyjęto odpowiedzi obejmujące wskazania {kluczowe; bardzo ważne; ważne} oraz za nieistotne wskazania {mało ważne; nieważne} uzyskano obraz zagrożeń przedstawiony na wykresie 38. Na szczególną uwagę zasługują wskazania jako nieistotne obejmujące kwestie zapamiętywania haseł w przeglądarkach internetowych (16%), instalowania oprogramowania z nieznanych źródeł (8%) oraz braku aktualnego oprogramowania antywirusowego (7%).

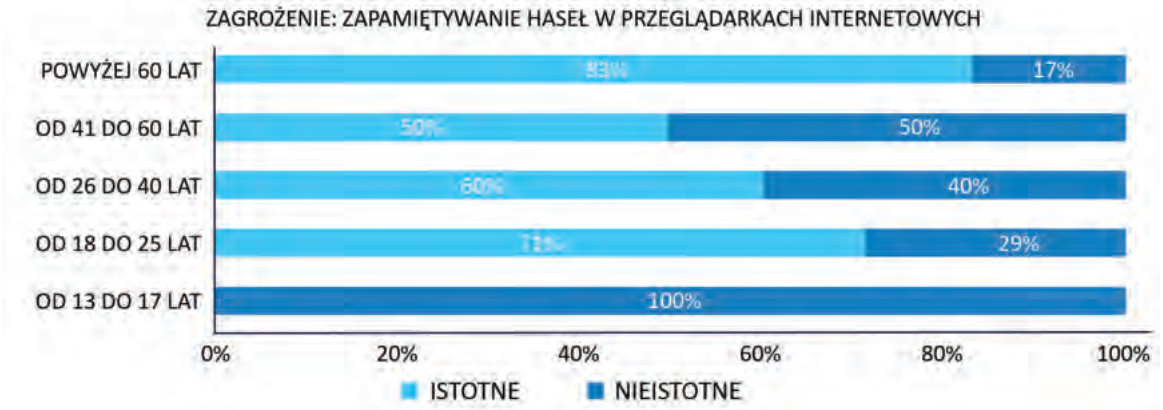
Dane prezentowane na wykresie 39 dotyczą zagrożenia związanego z zapamiętywaniem haseł w przeglądarkach internetowych i są alarmujące praktycznie w odniesieniu do każdej z grup wiekowych, przy czym, o ile najmłodsi nie przywiązują do tego zagrożenia



Wykres 37. Świadomość najpopularniejszych zagrożeń wśród respondentów



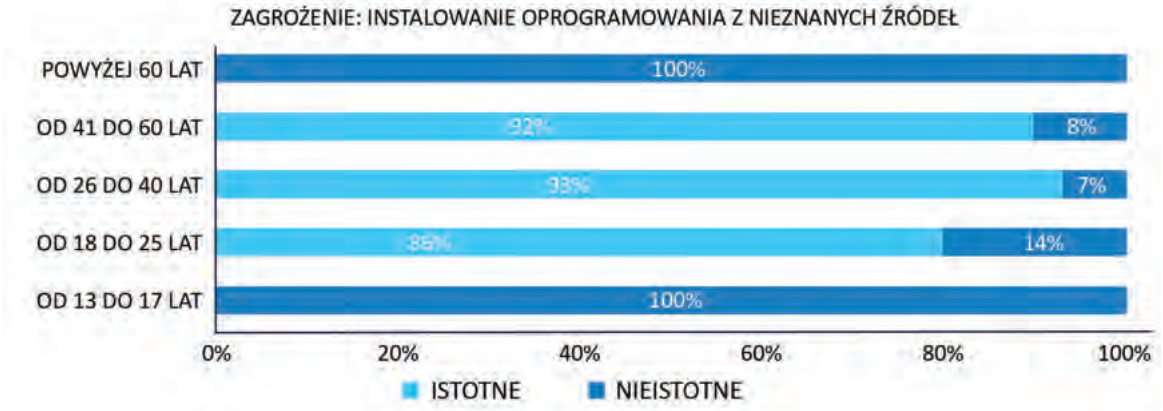
Wykres 38. Waga zagrożeń wg respondentów (górna ćwiartka)



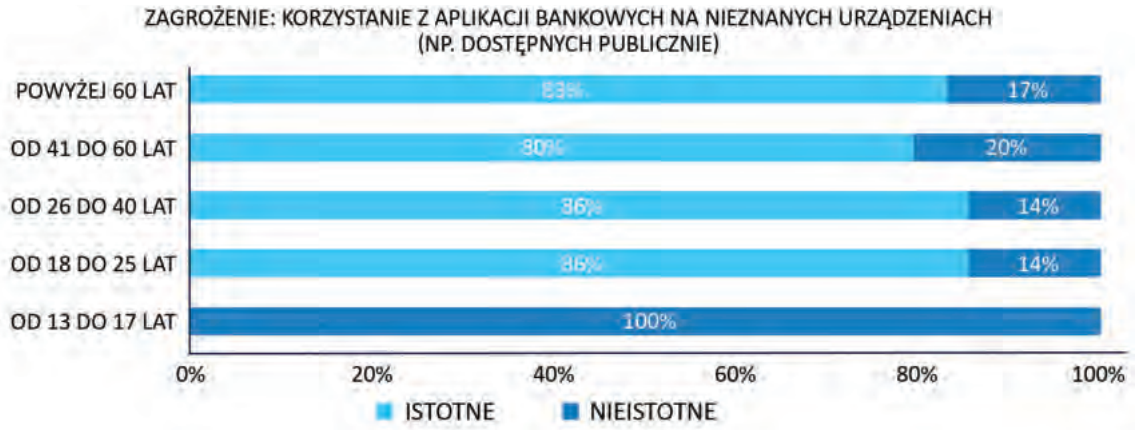
Wykres 39. Zagrożenie: Zapamiętywanie haseł w przeglądarkach internetowych a wiek

wagi, to najstarsi wykazują się największą powściągliwością.

W odniesieniu do zagrożeń związanych z instalacją oprogramowania z nieznanych źródeł, najmłodsi i najstarsi zdają się wiedzieć, że jest to działanie niosące za sobą wysokie ryzyko (patrz wykres 40). Co ciekawe, osoby w wieku od 18 do 25 lat w największej części traktują to jedno z podstawowych zagrożeń bezpieczeństwa jako nieistotne.



Wykres 40. Zagrożenie: Instalowanie oprogramowania z nieznanych źródeł a wiek



Wykres 41. Zagrożenie: Korzystanie z aplikacji bankowych na nieznanych urządzeniach (np. dostępnych publicznie) a wiek

W przypadku wykorzystania nieznanych urządzeń i wprowadzania na nich danych niezbędnych do rozpoczęcia pracy (ang. *authentication data*), brak świadomości zagrożenia widocznie rośnie wraz z wiekiem – patrz wykres 41. Jest to o tyle groźne zjawisko, iż w efekcie pozwala ewentualnemu świadomemu użytkownikowi odpowiednio przygotowanego urządzenia na zachowanie i w późniejszym czasie wykorzystanie zapisanych danych uwierzytelniających do systemów bankowych.

ROZDZIAŁ VI

PROGRAM ANALITYCZNO BADAWCZY

Wnioski i wyzwania

Rozdział ten stanowi podsumowanie raportu i skupia się na przedstawieniu wniosków końcowych. Został opracowany na podstawie całościowego, zebranego materiału badawczego i własnych przemyśleń autorów niniejszego opracowania.

Dedykowane podrozdziały mają na celu:

– Wskazanie rekomendacji w zakresie działań na rzecz poprawy bezpieczeństwa w środowisku bezpieczeństwa klienta bankowości elektronicznej.

– Predykcję zagrożeń w środowisku klienta bankowości elektronicznej i możliwych kierunków przeciwdziałania tym zagrożeniom.

Warto tutaj przywołać komentarz jednego z ekspertów, którzy brali udział w badaniu na potrzeby niniejszego raportu: *choć sektor bankowy generalnie oceniany jest jako wiodący w obszarze cyberbezpieczeństwa, to jest jednak niejednorodny. Są banki bardzo zaawansowane we wdrażaniu najlepszych standardów i dobrych praktyk, posiadają odpowiednie możliwości finansowe, pozwalające na wdrażanie odpowiednich zasobów IT, kadr i procesów, ale są też banki, które dokładnie z tych samych względów finansowych nie mogą sobie na to pozwolić. Jeśli do tego dodamy dużą konkurencję na rynku międzybankowym oraz konkurowanie banków z innymi podmiotami wchodzącymi na rynek usług płatniczych, a także niską świadomość klientów w zakresie bezpiecznego korzystania z usług płatniczych, to wówczas nasze pierwsze wrażenie może okazać się zbyt optymistyczne.*

6.1. Rekomendacje w zakresie działań na rzecz poprawy bezpieczeństwa w środowisku bezpieczeństwa klienta bankowości elektronicznej

6.1.1. Stosowanie jednolitej terminologii

Podstawowym problemem, który powoduje, że zrozumienie problematyki bezpieczeństwa bankowości elektronicznej może w niektórych przypadkach być istotnie utrudnione – zarówno dla klientów, jak i przedstawicieli branży – jest terminologia, a dokładnie nieprecyzyjne tłumaczenia określonych terminów i mylenie ich znaczeń. Przykładem może być tutaj „silne uwierzytelnianie klienta" (ang. *Strong Customer Authentication*), czyli termin wprowadzony przez dyrektywę PSD2, który oznacza potwierdzanie tożsamości oraz „autoryzacja" (ang. *authorization*), czyli wyrażanie zgody na przeprowadzenie transakcji. Obydwa terminy nie mogą być stosowane zastępczo w najróżniejszych opracowaniach branżowych lub procedurach bezpieczeństwa – ich znaczenie jest bowiem inne, pomimo tego, że podczas weryfikacji transakcji zarówno potwierdzając swoją tożsamość, jak i wyrażając zgodę na przeprowadzenie transakcji (autoryzując ją) zezwalamy na transfer środków pieniężnych.

6.1.2. Odejście od transakcji realizowanych z użyciem połączeń telefonicznych

W związku z istnieniem silnej podatności wśród klientów, a nawet i pracowników banków, związanej z wykorzystaniem ataków socjotechnicznych typu vishing, zaleca się całkowite odejście od transakcji realizowanych z użyciem połączeń telefonicznych (lub szerzej – głosowych). Konieczna jest tutaj także szersza edukacja w zakresie tego typu zagrożeń – nie chodzi bowiem o to, aby klienci wiedzieli, że tego typu ryzyko istnieje, ale dodatkowo mają także dokładnie wiedzieć, w jaki sposób postępować, czyli np. nie wykonywać poleceń dzwoniącego, przerwać połączenie, skontaktować się z bankiem za pomocą innego, oddzielnego kanału komunikacji (np. wizyta w placówce).

6.1.3. Wykrywanie podatności na urządzeniach końcowych

Eksperci rekomendują bankom wdrożenie i dalszy rozwój rozwiązań, które służą do wykrywania podatności na urządzeniach końcowych (komputer PC, laptop, tablet lub smartfon) – np. wykrywanie obecności na urządzeniu klienta oprogramowania typu AnyDesk lub TeamViewer, które przekazuje kontrolę nad pulpitem ofiary do osoby trzeciej (przestępcy).

Dodatkowo, banki powinny wymusić instalację na urządzeniach klientów oprogramowania zabezpieczającego, które będzie prowadziło monitoring behawioralny. Dzięki temu możliwe będzie zezwalanie na typowe operacje wykonywane na koncie bankowym przez użytkownika urządzenia (klienta bankowości elektronicznej) i blokowanie operacji, które pokrywają się ze schematem działania przestępców (np. są wykonywane przez boty zainstalowane na urządzeniu ofiary).

W przypadku rozwiązań do analizy behawioralnej rekomenduje się stosowanie algorytmów sztucznej inteligencji, co pozwoli efektywnej wykrywać anomalie w zachowaniu płatników lub użytkowników serwisów społecznościowych (np. Facebook).

6.1.4. Odejście od autoryzacji przez SMS

Eksperci rekomendują bankom odejście od autoryzacji przez SMS i wykorzystanie bezpieczniejszych metod weryfikacji transakcji. Jedna z propozycji zakłada szersze wykorzystanie biometrii, która, o ile jest

zaimplementowana prawidłowo, zapewnia wysokie bezpieczeństwo przy dużym komforcie użycia.

Doskonałą alternatywą dla rozwiązań biometrycznych lub kodów SMS są aplikacje uwierzytelniające Google Authenticator lub Microsoft Authenticator, które mogą generować kody jednorazowe dla określonej transakcji. Rozwiązania te są dostępne już dziś, a ich użycie nie wiąże się z istotnym przyrostem kosztów użycia aplikacji.

Jeżeli jednak z jakiegoś powodu konieczne jest użycie SMS, musi się to odbyć w taki sposób, aby klient wiedział, jak go wykorzystać i wyłącznie przy założeniu przestrzegania zasady faktycznej separacji kanałów komunikacji – w innym wypadku powstaje tutaj ryzyko związane np. z działaniem złośliwego oprogramowania, które będzie w stanie zebrać i wykorzystać wszystkie wymagane informacje dostarczane różnymi kanałami komunikacji na jedno urządzenie.

6.1.5. Lepsza kontrola nad płatnościami zbliżeniowymi realizowanymi z użyciem aplikacji mobilnych

Banki nie powinny zezwalać na dokonywanie płatności zbliżeniowych za pomocą aplikacji mobilnych, jeżeli nie zostanie zdjęta blokada ekranu urządzenia (np. za pomocą kodu PIN lub odcisku palca). Z kolei w przypadku, kiedy blokada ekranu na urządzeniu nie jest aktywna, aplikacja mobilna nie powinna w ogóle działać.

6.1.6. Badanie reakcji i utrwalanie właściwych zachowań na incydenty

Rekomenduje się budowanie odporności na zagrożenia wśród pracowników banków poprzez generowanie fałszywych incydentów przez zespoły odpowiedzialne za bezpieczeństwo. Takie działanie pozwala na badanie reakcji i utrwalanie właściwych zachowań (np. na phishing) w sposób całkowicie kontrolowany. Dzięki temu istotnie wzrastają szanse, że w kontekście prawdziwego zagrożenia pracownicy banku zadziałają prawidłowo.

Dodatkowym bardzo istotnym i według ekspertów pomijanym zagrożeniem jest brak procedur masowej obsługi incydentów zarówno w odniesieniu do klientów banku, jak i w przypadku wystąpienia incydentów w sieci wewnętrznej banku. Działy bezpieczeństwa funkcjonują w zależności od natężenia zdarzeń, zaś w przypadku znaczącego obciążenia, procedury są upraszczane do poziomu, który pozwala na podstawową zgodność z regulacjami prawnymi i ograniczanie zagrożeń w podstawowym zakresie, co w efekcie może prowadzić do znaczących strat zarówno po stronie banku, jak i klientów. Rekomenduje się uwzględnienie w procedurach bezpieczeństwa zdarzeń o charakterze masowym.

6.1.7. Symetryczna i ulepszona komunikacja z klientem

Komunikacja banku z klientem jest niesymetryczna – bank przekazuje klientowi tylko te informacje, które uważa za konieczne i tylko w takim zakresie, który jest wygodny dla banku. Powoduje to nie tylko przerzucenie odpowiedzialności i ryzyka na stronę klientów, lecz także stwarza pewien margines, w którym może powstawać dodatkowe ryzyko naruszeń bezpieczeństwa (w przypadku, gdy takie ryzyko ulegnie materializacji, banki często próbują obciążać pełną odpowiedzialnością klientów). Banki muszą przestać działać w trybie nakazowym, a powinny starać się wychowywać klientów – właśnie pod kątem bezpieczeństwa, a nie tylko oferty produktów i usług.

W związku z powyższym występuje problem braku relacji zaufania między klientem a bankiem (między słabszym a silniejszym). W celu naprawienia tej sytuacji rekomenduje się, aby komunikacja stała się bardziej prokliencka. Ze strony banku potrzebne jest tutaj większe zaangażowanie i pomoc w stosunku do klienta, przy czym nie chodzi tutaj o kolejne, rozległe dokumenty opisujące rzeczy istotne zdaniem banku i definiujące dodatkowe wymagania bezpieczeństwa, a o wyraźny, krótki i zrozumiały przekaz, jednoznacznie informujący: co, jak i dlaczego ma być zrobione po stronie klienta.

Postawienie na symetryczną i ulepszoną komunikację z klientem pozwoli bankom budować kulturę bezpieczeństwa bankowości elektronicznej. Ta kultura nie powinna być budowana przez każdy bank osobno, aby klienci nie zaczęli się gubić w rozmaitości zasad i standardów. Wydaje się, że rolę lidera mógłby pełnić tutaj Związek Banków Polskich – ma to być bowiem kultura bankowości elektronicznej, a nie kultura bankowości elektronicznej określonego banku. Ważne więc, aby budowa tej kultury nie poszła w kierunku opracowania kolejnej normy, bardziej istotna jest tutaj promocja wartości takich jak otwartość, współpraca i wzajemne zaufanie, czy też precyzyjna i możliwie uproszczona komunikacja z klientem (komunikaty typu: „co, jak i dlaczego?"). Istotny jest wreszcie wymóg, aby na każdym etapie pamiętać, iż elementami składowymi kultury bezpieczeństwa bankowości elektronicznej muszą zawsze być dwie strony: bank i klient. Obydwie strony muszą w ramach tej kultury współistnieć – klienci nie mogą mieć poczucia wykluczenia.

6.1.8. Wdrożenie rozwiązania typu „klient mówi: stop!"

Istotne jest także, aby klienci mieli możliwość szybkiego zgłaszania swoich podejrzeń odnośnie incydentów bezpieczeństwa, jeżeli zaobserwują jakieś anomalie, do dedykowanej komórki banku (chodzi tutaj o zespoły typu ABUSE – zajmujące się wszelkimi nadużyciami). Nie istnieją bowiem proklienckie procedury umożliwiające szybką komunikację w takiej sytuacji w celu np. natychmiastowej blokady przelewu w każdej postaci.

Oprócz konieczności stworzenia takich procedur, rekomenduje się także eliminację tzw. martwych stref, czyli okresów, w których kontakt z bankiem jest szczególnie utrudniony – np. w okresie od piątku, godz. 16:00 do poniedziałku, godz. 12:00. Takie martwe strefy nie tylko sprzyjają przestępczości, lecz także uniemożliwiają klientom zatrzymanie omyłkowych transakcji i ich następstw.

Docelowo chodzi o wytworzenie rozwiązania pozwalającego klientowi na natychmiastowe zablokowanie niechcianej transakcji w dowolnym momencie, które roboczo można by nazwać: „klient mówi: STOP!".

6.1.9. Dzienniki operacji wykonywanych na koncie powinny być dostępne dla klientów

Użytkownik powinien mieć możliwość sprawdzenia historii (dziennika) operacji wykonywanych na jego koncie, np. aby sprawdzić fakt logowania się z innych urządzeń niż zwykle przez niego używane, sprawdzić dane dotyczące uwierzytelniania i autoryzowania transakcji itd. Obecnie pełny obraz działań istnieje tylko po stronie banku. Sytuacją niedopuszczalną jest pobieranie przez bank opłat za przekazywanie informacji na temat operacji wykonywanych na koncie, co rodzi konflikty oparte o interpretację takiego stanu rzeczy: czy to faktycznie klient zdecydował, że nie chce takich informacji, czy może była to decyzja banku, aby przekazywanie informacji ograniczyć? Klient musi wiedzieć, co dzieje się na jego koncie, aby móc sprawnie reagować.

6.1.10. Wymuszanie spełniania wymagań bezpieczeństwa

Banki powinny nie tylko definiować wymagania odnośnie bezpieczeństwa, lecz także brać czynny udział w wymuszaniu ich spełniania – jeżeli klient nie spełnia jakiegoś wymagania, np. nie ma włączonej blokady ekranu na smartfonie lub nie następuje okresowa zmiana hasła, to nie może korzystać z aplikacji mobilnej do bankowości elektronicznej. Wszelkie wymagania muszą być jednak dla klientów zrozumiałe, co do celowości ich wdrożenia.

6.1.11. Szersze użycie rozwiązań opartych o tokeny

Banki powinny w większym zakresie korzystać z generatorów tokenów, takich jak Google Authenticator i Microsoft Authenticator, co pozwoli odejść od stałego atrybutu bezpieczeństwa (np. stałe, niezmieniane hasło). Tokeny są bardziej bezpieczne i wygodne, ponieważ generowane są automatycznie i regularnie. Wdrożenie rozwiązań, takich jak Google Authenticator lub Microsoft Atuhenticator, nie niesie istotnych, dodatkowych kosztów.

6.1.12. Właściwa architektura aplikacji mobilnych

Rekomenduje się, aby banki zwracały uwagę na właściwą architekturę aplikacji mobilnych – ma to zagwarantować taką ich budowę, aby zużywały jak najmniej zasobów urządzenia, na którym są uruchomione. Optymalnie, żeby tego typu aplikacje używały środowisk zwirtualizowanych (koncepcja separacji zasobów – „sandbox"). Dzięki właściwej architekturze i uwzględnieniu koncepcji separacji zasobów, potencjalny wpływ na działanie aplikacji mobilnej, jak również komunikacja aplikacji ze światem zewnętrznym, będą zminimalizowane w przypadku incydentów związanych z bezpieczeństwem.

6.1.13. Właściwe testowanie rozwiązań

W ocenie ekspertów bezpieczeństwo traktowane jest przede wszystkim jako bezpieczeństwo w zakresie prawnym i zgodność z regulacjami instytucji nadzorujących.

W przypadku niektórych narzędzi do przygotowywania aplikacji dostępne są takie rozwiązania, jak SDL (ang. *Security Development Lifecycle* – proces tworzenia bezpiecznego oprogramowania), które umożliwiają weryfikację i przeprowadzenie testów odporności aplikacji na współczesne modele zagrożeń. Ważne, aby takie testy były faktycznie przeprowadzane.

Zaleca się także szczegółową analizę kodu w przypadku korzystania z ogólnie dostępnych bibliotek, jak również analizę tych bibliotek w razie ich aktualizacji w sytuacji aktualizacji oprogramowania bazowego.

W ocenie ekspertów na etapie budowy i testowania oprogramowania nie można pominąć możliwych ataków związanych ze sterownikami urządzeń, które w ostatnim czasie stanowią pole do rozwoju możliwych zagrożeń.

Rozwiązania powinny być testowane nie tylko pod kątem podatności i bezpieczeństwa, lecz przede wszystkim testy powinny odbywać się w środowisku

i w warunkach, w jakich rozwiązanie jest przez klienta wykorzystywane.

6.1.14. Migracja do TLS 1.3 i lepsza kryptografia

Ze względu na podatności protokołu kryptograficznego TLS zaleca się szybką migrację do wersji 1.3. Na rynku wciąż znajdują się serwisy zabezpieczone starszą wersją TLS 1.2.

W kryptografii obowiązuje zasada, że szyfry strumieniowe nie chronią nas pełną długością klucza, a tylko połową jego długości. Istotne jest „bit security", czyli określenie, ile efektywnie bitów klucza nas faktycznie chroni. Analizując komunikację, jeden z ekspertów wskazał, że większość banków używa wciąż szyfrowania AES-128GCM (ang. *Advanced Encryption Standard* – zaawansowany standard szyfrowania), co rodzi pytanie, czy 64 bity zapewnia odpowiedni poziom ochrony – nawet biorąc pod uwagę użycie metody GCM (ang. *Galois Counter Mode*), czyli uwierzytelniania krzywych eliptycznych.

Warto zauważyć, że w „Commercial National Security Algorithm Suite" („Komercyjny zestaw algorytmów bezpieczeństwa narodowego" – tł. własne)[45] NSA (ang. *National Security Agency* – agencja bezpieczeństwa narodowego, odpowiedzialna w USA, m.in. za wywiad elektroniczny) już w 2015 r. postulowała konieczność wdrożenia algorytmów odpornych na złamanie z wykorzystaniem technologii komputerów kwantowych – wskazywano tam wówczas AES-256.

W przypadku podjęcia decyzji o przeniesieniu szyfrowania w świat funkcji eliptycznych, pozostaje kwestia krzywych eliptycznych i ich parametrów, które będą stosowane. Teoretycznie każdy może wyliczyć parametry krzywej eliptycznej. Zły dobór parametrów powoduje jednak, że szyfrowanie na krzywych eliptycznych staje się niebezpieczne – np. liczba kardynalna pola jest za niska, czyli punkty na krzywych eliptycznych zbyt szybko się powtarzają, czy też pojawiają się zależności czasowe umożliwiające atak kanałem podprogowym. Sprawdza się tutaj zasada, że amatorzy nie powinni implementować algorytmów kryptograficznych.

W związku z powyższym zaleca się przegląd używanych rozwiązań w zakresie kryptografii i dostosowanie ich do wyzwań przyszłości (mając na uwadze np. rozwój technologii komputerów kwantowych) przy wsparciu ekspertów w dziedzinie szyfrowania.

6.1.15. Wprowadzenie okresów przejściowych dla nowych rozwiązań

Banki powinny rozważyć stosowanie okresów przejściowych w przypadku wdrażania nowych rozwiązań. Jeżeli od długiego czasu klienci mieli możliwość wykorzystania rozwiązania A (starszego), a z jakichś powodów bank wprowadza rozwiązanie B (nowsze), to okres przejściowy ma klientom dać szansę, aby przystosowali się do zmiany.

Istotny jest tutaj atrybut dostępności (ang. *availability*), który obok poufności (ang. *confidentiality*) i spójności (ang. *integrity*) stanowi jedną z podstawowych cech bezpieczeństwa usług bankowych. Przykładem może być wprowadzenie nowej wersji aplikacji mobilnej, która od klienta wymagać będzie zakupu nowego smartfonu działającego w oparciu o wspieraną przez dostawcę aplikacji wersję systemu operacyjnego. Klient zmuszony jest tutaj do poniesienia kosztu zakupu nowego urządzenia, co może wymagać czasu, a w przypadku, kiedy nie będzie istniał okres przejściowy, natychmiastowo utraci możliwość wykorzystania starej wersji aplikacji mobilnej, czyli usługa stanie się dla niego niedostępna.

6.1.16. Budowa ekosystemu sprzyjającego bezpieczeństwu finansów elektronicznych

W tym wymiarze kluczowe są wspólne działania zarówno platform FinTech-owych, jak i banków oraz producentów rozwiązań. Powstać musi cały ekosystem składający się z banków, instytucji finansowych, organów kontrolnych i nadzorujących, takich jak np. Komisja Nadzoru Finansowego (KNF) w Polsce, które wspólnie będą kooperować na rzecz bezpieczeństwa finansów elektronicznych.

KNF powinien pełnić tutaj rolę wiodącą, ponieważ wydaje rekomendacje techniczne dotyczące zarówno platform przetwarzania danych w systemach bankowych, jak i w zasobach chmurowych (ang. *cloud computing*) oraz rekomendacje techniczne dotyczące bankowości i infrastruktury finansowej. Przede wszystkim jednak KNF – jako organ kontrolny i nadzorujący – jest w stanie wyegzekwować od banków i innych instytucji finansowych faktyczne wdrożenie konkretnych rozwiązań technicznych. Warto podkreślić, że organ kontroli i nadzoru w danym państwie, np. KNF w Polsce, wymieniając informacje w ramach Europy i na płaszczyźnie międzynarodowej, posiada zdolność monitorowania trendów w zakresie najbardziej aktualnych zagrożeń i podatności, które są najczęściej wykorzystywane do nadużyć w systemach bankowości elektronicznej.

W ramach ekosystemu sprzyjającego bezpieczeństwu finansów elektronicznych istotna jest także

[45] *Commercial National Security Algorithm Suite*, https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm, stan z dn. 8 sierpnia 2021.

edukacja – rozumiana jako ciągła praca nad klientem, która ma sprzyjać nie tylko budowie świadomości zagrożeń, lecz również zwiększeniu realnej odporności na działania przestępcze. Chodzi więc o wspólne działania organów kontroli i nadzoru, instytucji finansowych i producentów na rzecz takiej właśnie edukacji, w tym o promocję działań edukacyjnych w zakresie bezpieczeństwa finansów elektronicznych.

W ocenie ekspertów, uzależnienie finansów w wymiarze podstawowym od rozwiązań elektronicznych prowadzi do stanu, w którym w razie braku dostępu do sieci niemożliwym może stać się zaspokojenie podstawowych potrzeb klientów banku (np. zakup chleba, wody czy też innych produktów pierwszej potrzeby.) Niezbędnym jest mitygacja tego zagrożenia i wprowadzenie rozwiązań, które pozwolą docelowo na pracę w trybie off-line.

Należy zauważyć, że wprowadzanie wszelkich rozwiązań mających na celu budowanie ekosystemu musi odbywać się przy założeniu możliwie najniższych kosztów po stronie klientów.

6.1.17. Lepsza współpraca i komunikacja pomiędzy policją a bankami

Typowa współpraca wygląda tak, że biegły sugeruje policjantowi, o jakie dane powinien poprosić bank w przypadku wykrycia przestępstwa, lecz banki nie reagują tutaj zbyt przychylnie – dostarczają bowiem bezwzględne minimum danych, co utrudnia pracę Policji. Do pewnego stopnia można ten fakt usprawiedliwić rzeczywistością prawną, m.in. także tajemnicą bankową oraz obawami banków, które nie chcą ujawniać zbyt wiele danych związanych z przestępczością z troski o swoją reputację. Takie podejście jest jednak błędne. Mimo wszystko, musi w obszarze zapobiegania i zwalczania przestępczości istnieć silna świadomość, że bez udziału banków żadni biegli, ani Policja nie są w stanie poradzić sobie z przestępczością.

Niektórzy eksperci podkreślali fakt, że nie istnieje prawo, które wspierałoby banki w zakresie wykrywania, analizowania i przeciwdziałania przestępstwom popełnianym na szkodę banków lub ich klientów. Brakuje też odpowiednich przepisów, np. w zakresie uprawnień dotyczących wymiany pomiędzy różnymi sektorami informacji stanowiących tajemnice prawnie chronione, które wspierałyby banki i organy ścigania zwalczające przestępczość bankową.

Wbrew wszelkim utrudnieniom rekomenduje się więc wspólne działanie biegłych, Policji i banków na rzecz skutecznego zwalczania przestępczości bankowej. Od lat istnieje bowiem problem komunikacyjny pomiędzy Policją a bankami, pomimo dotychczasowych podejmowanych inicjatyw.

6.2. Predykcja zagrożeń w środowisku klienta bankowości elektronicznej i możliwych kierunków przeciwdziałania tym zagrożeniom

Niniejszy rozdział ma na celu wskazanie potencjalnych zagrożeń środowiska klienta bankowości elektronicznej w przyszłości. Warto tutaj przywołać słowa jednego z ekspertów, z którym przeprowadzono wywiad – zwrócił on uwagę, że rozwój technologiczny banku powinien mieć na uwadze obszar bezpieczeństwa, bowiem na tym polu odbywa się swoisty wyścig między przestępcami a bankami, przy czym celem niekoniecznie jest to, aby przestępcy pozostawali w tyle, bo ten stan rzeczy jest prawdopodobnie niemożliwy do osiągnięcia, lecz chodzi o podejmowanie takich decyzji i kierunków rozwoju, aby nie pozwolić uciec im zbyt daleko.

6.2.1. Kwestionowanie autoryzacji potencjalnie zmanipulowanych transakcji

Ciekawym problemem, na który uwagę zwrócili eksperci, jest kwestia świadomej autoryzacji transakcji. Chodzi tutaj o zdolność do uzyskania bezdyskusyjnej odpowiedzi na pytanie: czy klient autoryzujący jakieś działanie (np. transakcję przestępczą) miał niezaburzoną świadomość tego, co robi, czy też pod wpływem oddziaływania socjotechnicznego (manipulacji) jego percepcja została zmieniona przez przestępców?

Zadanie nie wydaje się trywialne, ponieważ trudne będzie w takim przypadku nie tylko ustalenie stanu faktycznego, lecz należy mieć również świadomość, że konkretna odpowiedź będzie miała przełożenie na ogólną ocenę znaczenia (wręcz ważności) konkretnego aktu autoryzacji. Dostrzec można więc zagrożenie związane z kwestionowaniem ważności autoryzacji przez potencjalnie zmanipulowanych klientów.

6.2.2. Komputery kwantowe, waluty cyfrowe i sztuczna inteligencja

W kontekście transformacji cyfrowej należy podkreślić potencjał komputerów kwantowych. Wydaje się mało prawdopodobne, aby w najbliższym czasie tego typu sprzęt mógł być stosowany przez przeciętnych przestępców. Jeżeli jednak uświadomimy sobie, że to państwa są najpotężniejszymi aktorami cyberzagrożeń, mają odpowiednie zaplecze kapitału finansowego i technicznego, a do tego są w stanie prowadzić badania na własną rękę i zapewnić współpracującym z nimi przestępcom nie tylko dostęp do najnowszych

technologii czy dobre wynagrodzenie, ale i ochronę przed międzynarodowymi organami ścigania, to ryzyko okazuje się bardziej realne.

Przedstawione obawy w tym zakresie można uzupełnić słowami prof. Marco Gercke z Uniwersytetu w Kolonii, który jest szefem niemieckiego Instytutu Badań nad Cyberprzestępczością[46] (ang. *Cybercrime Research Institute): „Jeśli tempo rozwoju komputerów kwantowych zostanie utrzymane (przekroczono już barierę już 50 kubitów) ma to potencjał, aby zakończyć skuteczność obecnie stosowanych metod szyfrowania w ciągu najbliższych pięciu lat. W tym samym czasie jest prawdopodobne, że chociaż sztuczna inteligencja nie będzie w stanie w pełni zrównać się z mocnymi stronami człowieka, przewyższy to, co jest konieczne, aby wykorzystać ludzkie słabości. W konsekwencji najprawdopodobniej zobaczymy coraz większe wykorzystanie sztucznej inteligencji w tych obszarach przestępczości, gdzie obecnie nie jest wykorzystywana"*[47].

Na uwagę zasługują także słowa prof. Babaka Akhgara, dyrektora Centric UK: *„Globalna absorpcja walut cyfrowych w połączeniu z proliferacją aplikacji opartych na sztucznej inteligencji, stopniowo staje się głównym środkiem wymiany towarów i usług. Kluczowym wyzwaniem dla organów ścigania i pozostałych interesariuszy, takich jak krajowe lub międzynarodowe władze oraz przedstawiciele sektora usług finansowych, jest ochrona społeczeństwa i gospodarki wobec pełnego spektrum przestępstw z wykorzystaniem sztucznej inteligencji i walut cyfrowych (…)"*[48].

Należy również przytoczyć technologie związane z imitacją (ang. *deep fake* – tł. własne: głęboka imitacja), które pozwalają tworzyć fałszywe wizerunki – w postaci ruchomych obrazów i głosu – osób wpływowych (np. polityków, reprezentantów instytucji finansowych itp.) za pomocą algorytmów sztucznej inteligencji. Przestępcy mogą użyć tak wygenerowanych materiałów do obchodzenia systemów uwierzytelniania i autoryzacji oraz wyłudzeń lub oszustw. Dobrym przykładem jest tutaj przestępstwo, którego dokonano przy użyciu podrobionego głosu członka zarządu jednej z niemieckich firm. Dyrektor generalny (ang. *Chief Executive Officer, CEO)* brytyjskiej firmy związanej z rynkiem energetycznym w wyniku ataku socjotechnicznego zlecił dokonanie przelewu kwoty w wysokości 220 000 EUR do banku na Węgrzech, ponieważ był przekonany, że rozmawia przez telefon z prawdziwą osobą, a sprawa jest pilna. Oszuści na tyle dobrze podrobili głos wydającego polecenie, że ofiara rozpoznała w nim lekki niemiecki akcent i charakterystyczną melodię głosu na co dzień znanej jej osoby[49].

Socjotechnika używana przez przestępców jest bardzo skuteczna – klienci dają się złapać na klasyczne metody oddziaływania, np. presję czasu (konieczność szybkiego podjęcia decyzji, której oczekują przestępcy). Wszelkie techniki manipulacyjne, dodatkowo wsparte zaawansowanymi technologiami, zdają się stanowić największe zagrożenie – najsłabszym i najbardziej podatnym na przestępcze oddziaływanie ogniwem pozostaje człowiek. Jedyną metodą wzmocnienia odporności czynnika ludzkiego jest ciągła, szeroko zakrojona edukacja na temat zagrożeń, prawdopodobieństwa ich wystąpienia i sposobów minimalizacji ryzyka w obszarze bankowości elektronicznej – szczególnie mając na uwadze postępujący proces cyfryzacji praktycznie wszystkich dziedzin naszego życia.

Wydaje się więc, że prawdziwe wyzwania dla bezpieczeństwa bankowości elektronicznej w przyszłości znajdują się na styku ludzkich podatności, słabości i rozwoju zaawansowanych technologii, w których pokładamy obecnie największe nadzieje. Otwartym pozostaje pytanie, na ile przewidywania ekspertów branżowych i naukowców okażą się słuszne.

[46] Instytut Badań nad Cyberprzestępczością, strona główna: http://cybercrime.de/.

[47] *Internet Organised Crime Threat Assessment (IOCTA) 2019*, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, stan z dn. 9 sierpnia 2021, s. 58.

[48] *Internet Organised Crime Threat Assessment (IOCTA) 2019*, https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf, stan z dn. 9 sierpnia 2021, s. 55.

[49] C. Stupp, Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, stan z dn. 11 stycznia 2021.

Spis wykresów

Spis fotografii

Spis rycin

Spis schematów

Raport przygotowany na zlecenie Fundacji
Warszawski Instytut Bankowości

PROGRAM
ANALITYCZNO
BADAWCZY