ŚWIAT BANKOWOŚCI SPÓŁDZIELCZEJ
NR 1/611 STYCZEŃ – MARZEC 2024
ISSN 2719-4515

BANK SPÓŁDZIELCZY

Nowoczesny bank:
nie tylko konto, kredyt i lokata

rozmowa z Jackiem Zacharewiczem
Prezesem ESBANKU BS

s. 7

PODCAST SPÓŁDZIELCZY SGB

Cyberbezpieczeństwo
i usługi IT w SGB

s. 11

Rok Edukacji
Ekonomicznej 2024

s. 39

BS

OD REDAKCJI

GDZIE PRAWDA,
GDZIE FIKCJA?

Coraz trudniej odróżnić co jest prawdą, a co fikcją. Codziennie spotykamy się z tysiącami komunikatów, które często są nieprawdziwe i zmanipulowane.

Pod względem technologicznym jesteśmy bardzo dobrze zabezpieczeni. Najnowszy ranking National Cyber Security Index (NCSI), który mierzy poziom cyberbezpieczeństwa państw, uplasował nasz kraj – UWAGA! – na pierwszym miejscu na świecie. Raport ocenia też zdolność do zarządzania sytuacjami kryzysowymi w IT. Rozmawiałem o raporcie z jednym z prezesów dużej firmy. Powiedział, że wolałby, żebyśmy byli niżej, ponieważ czasem tak dobry wynik powoduje rozluźnienie i może sprawić, że tracimy czujność. A w sferze bezpieczeństwa cybernetycznego trzeba zawsze pracować na najwyższych obrotach...

Tematem numeru jest technologia, cyberbezpieczeństwo i usługi jakie oferuje SGB. Jak działają Banki Spółdzielcze SGB wspólnie z bankiem zrzeszającym? SGB-Bank oferuje szerokie spektrum usług zabezpieczających banki spółdzielcze przed przestępczością elektroniczną. Temat przybliża Daniel Krzywiec, dyrektor Departamentu Cyberbezpieczeństwa w SGB-Banku.

Bezpieczeństwo jest dla nas podstawowym warunkiem rozwoju usług bankowości internetowej i mobilnej. Wdrożone rozwiązania umożliwiają wykrywanie anomalii na rachunku klienta, blokowanie kanałów dostępu oraz zrywanie podejrzanych sesji – stwierdza szef bezpieczeństwa.

Wtóruje mu Piotr Mazur, dyrektor Departamentu Informatyki w SGB-Banku. Autor w swoim artykule przygląda się kluczowym aspektom i najlepszym praktykom związanym z bezpieczeństwem dostępu do sieci w bankach.

Jak wspomniałem na wstępie, cyfrowo jesteśmy zabezpieczeni. Jednak sama technologia bez wsparcia człowieka, jego edukacji i uczulenia na niebezpieczeństwa, warta jest niewiele. Zwłaszcza, gdy przestępcy korzystają z najnowszych osiągnięć socjotechniki, psychologii, sztucznej inteligencji, wiedzy informatycznej i narzędzi cyfrowych. Dziś potrzebujemy i technologii i zdrowego rozsądku oraz edukacji.

Mierzymy się z coraz bardziej wyrafinowanymi socjotechnikami, które mają na celu wyciągnięcie od nas poufnych danych i uzyskanie dostępu do naszych kont. Z drugiej strony wiedza finansowa wielu naszych rodaków pozostawia wiele do życzenia. Dlatego też sektor bankowości spółdzielczej nie tylko dba o bezpieczeństwo finansowe swoich klientów, ale również edukuje i wspiera. Rozwój technologii, wykorzystanie sztucznej inteligencji, nowe usługi dostępne poprzez kanały zdalne, to tylko niektóre możliwości, jakie oferują Banki Spółdzielcze SGB. Ale mimo to nie tracą swojego lokalnego charakteru i podejścia do klienta. Potwierdza to rozmowa Arlety Węgrzyńskiej z Jackiem Zacharewiczem, prezesem Zarządu ESBANKU Banku Spółdzielczego w Radomsku.

Kluczem do sukcesu jest dywersyfikacja kanałów obsługi. Bez wątpienia trend digitalizacji usług bankowych oraz cyfryzacji klientów każdego dnia nabiera tempa, a Mobilne Przyspieszenie SGB, którego ESBANK jest aktywnym uczestnikiem, to konieczność. Wychodząc z tego założenia, już w 2012 r. udostępniliśmy swoim klientom własną aplikację mobilną. Jednak żadna technologia nie zastąpi w pełni kontaktu z drugim człowiekiem – mówi prezes J. Zacharewicz. I trudno się z tą tezą nie zgodzić. Bezpośrednie kontakty w biznesie, osobiste spotkania to atuty, które mają banki spółdzielcze. Ich rola polega na zaspokajaniu potrzeb finansowych klientów, wspieraniu inicjatyw ważnych dla lokalnych społeczności, a także na edukowaniu. Edukacja ekonomiczna jest niezmiernie ważna. Dlaczego? 35% Polaków w wieku do 34 lat uważa, że jeśli w budżecie państwa brakuje pieniędzy, to należy je dodrukować, by uzupełnić lukę. To jedna z zaskakujących danych, którą można znaleźć w raporcie z ogólnopolskiego panelu badawczego Ariadna.

Czy wiedzę ekonomiczną można propagować? Można i trzeba. Sektor spółdzielczy dołączył do ogólnopolskiej akcji Rok Edukacji Ekonomicznej 2024. Senat RP ustanowił rok 2024 rokiem edukacji ekonomicznej. Czy ten projekt jest nam rzeczywiście potrzebny? Na to pytania odpowiada Ewelina Ignaczak, dyrektorka Biura Marketingu i Komunikacji w SGB-Banku.

O narodowym, ogólnopolskim programie mającym na celu poszerzanie wiedzy finansowej Polaków dla naszego e-magazynu „Bank Spółdzielczy" wypowiadają się m.in. Małgorzata Kidawa-Błońska i Jan Grzesiek. W tej edukacji nie tylko ważne jest zarządzanie własnym budżetem, ale również wiedza, jak chronić swoje pieniądze. Swoją wiedzą w tej dziedzinie dzieli się także Andrzej Borowiak.

Poza próbami wyciągania od nas danych coraz powszechniejsza jest dezinformacja, czyli fake newsy. Polecam tekst Agnieszki Szelejewskiej: – *Naszym najlepszym sprzymierzeńcem w walce z dezinformacją jest fact-checking, czyli metoda dociekania prawdy poprzez przeszukiwanie wiarygodnych źródeł, dokumentów, danych statystycznych, badań naukowych itp.* – przekonuje autorka.

W SGB dokładamy wszelkich starań, by nasi klienci czuli się bezpiecznie. Rozwijamy nowe usługi i produkty. Banki Spółdzielcze SGB ostatnio wprowadziły usługę monitoringu kart – kolejne narzędzie w wojnie z cyberprzestępcami…

Co jeszcze w naszym magazynie? Jak zwykle dużo rozmów, ciekawej publicystyki, porad prawnych i… trochę tematów związanych z muzyką, książką i filmem.

Piszę ten wstępny artykuł w sobotnie przedpołudnie, siedząc w niewielkiej kawiarence Klif w Trzęsaczu. Mam widok na ruiny kościoła i Bałtyk. Święci słońce, lekko wieje wiatr. Czuć wiosnę w powietrzu. Aż chce się żyć!

Życzę Państwu dużo wiosennej energii! Dobrej lektury.

Roman Szewczyk
Redaktor Naczelny

BANK SPÓŁDZIELCZY
Adres Redakcji: Szarych Szeregów 23a, 60-462 Poznań,
M.: **505 459 471**, E.: **wydawnictwo@bodie.pl,**
www.bodie.pl/szkolenia/bodie-extra/wydawnictwo/ksiazki
Redaguje zespół: redaktor naczelny – **Roman Szewczyk**
Redaktorzy prowadzący – **Rafał Łopka, Jerzy Sygidus**
Redakcja techniczna – **BODiE**
Korekta: **Jerzy Sygidus**
Reklama: **Monika Zarębska – BODiE,** M.: +48 608 339 937
Projekt: **dubielstudio.pl, rm2.eu** Skład: **Drukma**
Stale współpracują: **Robert Azembski, Andrzej Borowiak, Janusz Orłowski, Robert Woźniak**
Współpraca podcast: **Michał Kocurek, Katarzyna Miler**

Zdjęcie na okładce: **Archiwum ESBANK BS**
Obróbka: **dubielstudio.pl**
Zdjęcia we wnętrzu pochodzą z **Pixabay.com**, **Unsplash.com i shutterstock.com**.
Wydawca: **Bankowy Ośrodek Doradztwa i Edukacji Sp. z o.o.**
Szarych Szeregów 23a, 60-462 Poznań, M.: 505 459 471,
E.: wydawnictwo@bodie.pl
Na zlecenie SGB-Banku SA

BS
NA RYNKU OD 1964 ROKU

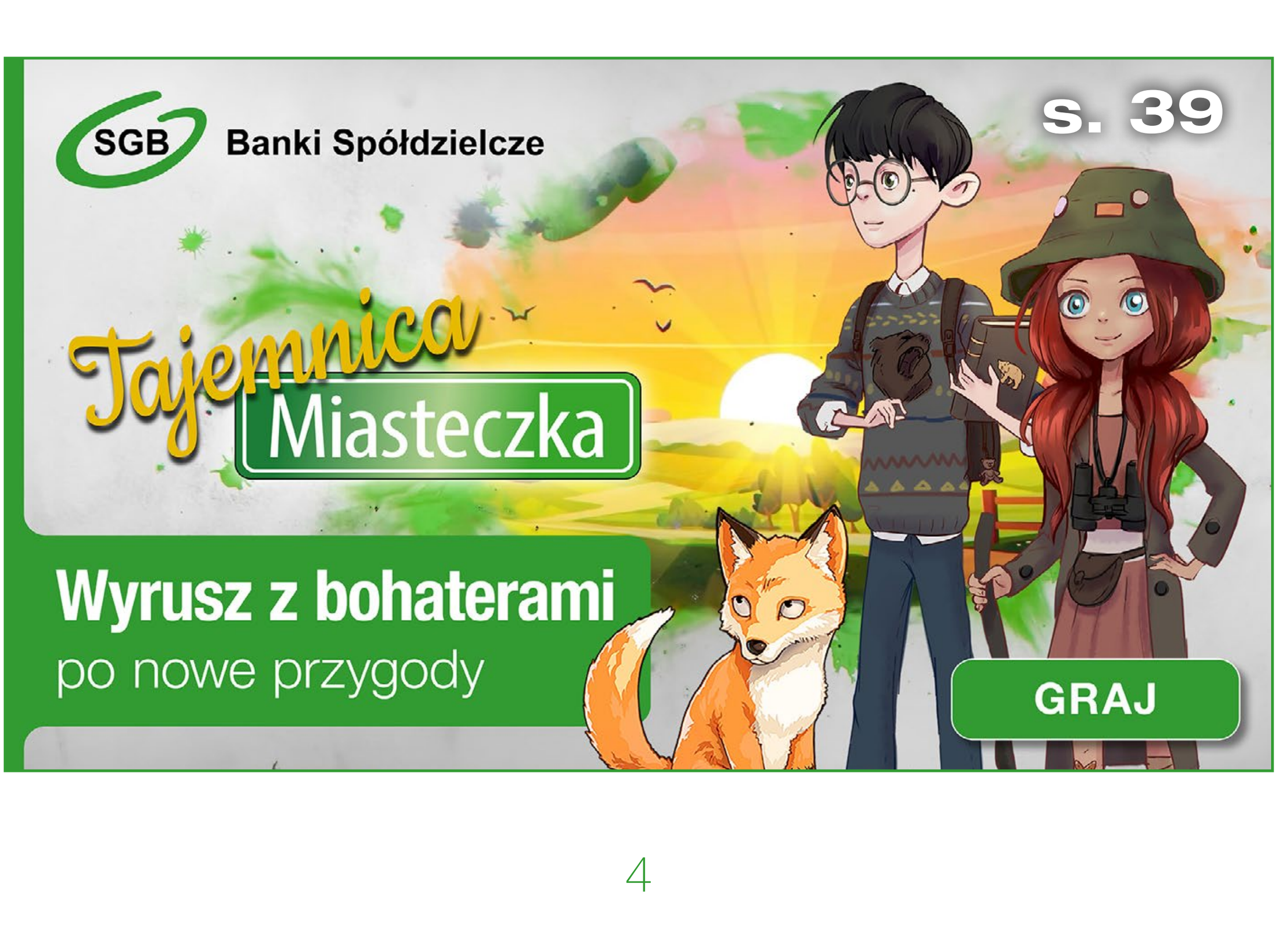
BS

SPIS TREŚCI

BS

SPIS TREŚCI

KLIKNIJ ŻEBY PRZEJŚĆ DO ARTYKUŁU



DLACZEGO PRZEDSIĘBIORCY WYBIERAJĄ BANKI SPÓŁDZIELCZE SGB?

WYSTARTOWAŁA KOLEJNA KAMPANIA SGB

Rozpoczynamy kolejny etap działań promujących markę Banki Spółdzielcze SGB. Konsekwentnie skupiamy się w nim na wartościach, które stoją za naszą codzienną pracą. Tym razem nowa kampania SGB dotyczy klientów firmowych, którzy w Bankach Spółdzielczych SGB mają partnera profesjonalnego, zaufanego i takiego, którego się po prostu lubi.

Hanna Kniołek
SGB-Bank SA

Rafał Łopka
SGB-Bank SA

Nowa kampania, która została zrealizowana razem z agencją reklamową GPD Agency oraz GPD Studio, potrwa do końca czerwca. Spot – w pełnej 30” wersji, skrót 15” oraz trzy skróty internetowe 6” – można zobaczyć w telewizji (TVP i TVN), internecie, TVP VOD, TVN Player i Polsat Box. Reżyserem jest, tak jak w poprzednich latach, Łukasz Korczak.

W spotach reklamowych znana z wcześniejszych kampanii dziennikarka spotyka się tym razem z przedsiębiorcami. Na zadane przez nią pytanie: „Dlaczego przedsiębiorcy wybierają Banki Spółdzielcze SGB” odpowiadają bohaterowie spotu, którzy cenią je za to, że znają potrzeby lokalnych przedsiębiorców, wpierają inwestycje blisko i daleko oraz mają doradców na których mogą liczyć.

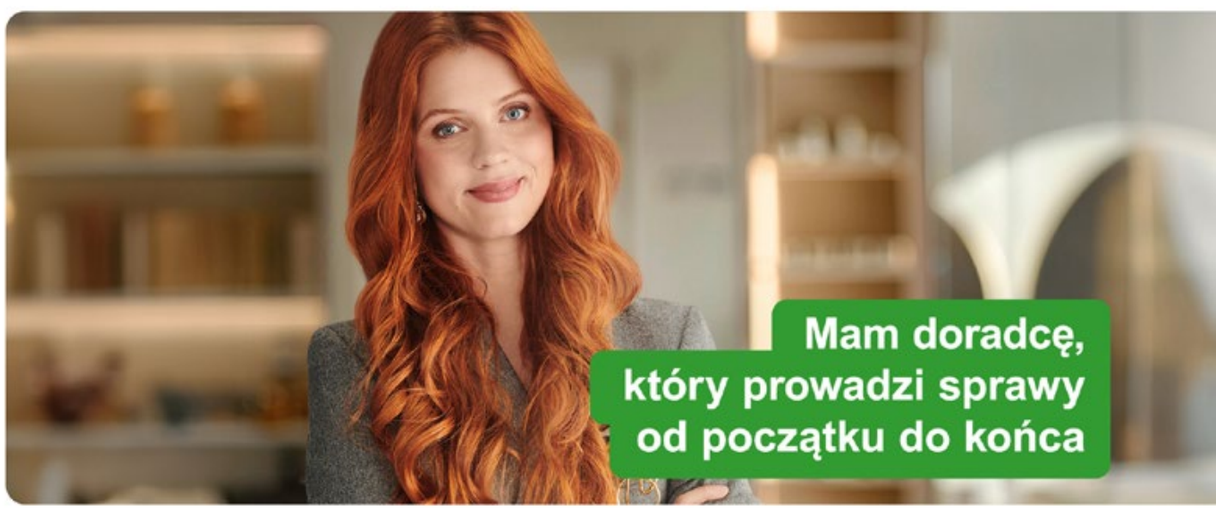
Film można obejrzeć na oficjalnym kanale SGB na YouTube:
https://youtu.be/Q4uvpwzXN-4

Kampania dla przedsiębiorców pokazuje, jak ważni dla nas są ludzie i relacje, które budujemy w lokalnych społecznościach, ale też biznes, który wspieramy. Zgodnie z hasłem: „Dobrze dbać o siebie nawzajem” – zaznacza Ewelina Ignaczak, dyrektorka Biura Marketingu i Komunikacji w SGB-Banku. – *Właśnie z uwagi na to jak ważne są dla nas relacje, doceniamy to, że kolejny projekt udaje nam się realizować z tym samym zespołem. Bo dobre relacje to dobre zrozumienie i ogromny komfort pracy. Bo że też świetne efekty, to już Państwo zobaczą sami* – dodaje.

Do zadań GPD należały m.in. produkcja i postprodukcja spotu oraz sesja foto. Do stworzenia spotu wykorzystano najnowocześniejsze narzędzia AI.

Więcej informacji na stronie **takaroznica.sgb.pl**

A jeśli ktoś chciałby zajrzeć za kulisy powstania naszego spotu, to zapraszamy!
https://www.youtube.com/watch?v=meFd _ igfuOg



Banki Spółdzielcze SGB dla firm

SGB Banki Spółdzielcze

NOWOCZESNY BANK: nie tylko konto, kredyt i lokata

FOT. ARCHIWUM ESBANK BS

Rozmowa z **Jackiem Zacharewiczem**, prezesem Zarządu ESBANKU Banku Spółdzielczego z siedzibą w Radomsku

Kilka dni temu bank otworzył placówkę w Częstochowie w nowej lokalizacji. Czy w dobie bankowości mobilnej warto jeszcze utrzymywać tradycyjne placówki bankowe?

Kluczem do sukcesu jest dywersyfikacja kanałów obsługi. Bez wątpienia trend digitalizacji usług bankowych oraz cyfryzacji klientów każdego dnia nabiera tempa, a Mobilne Przyspieszenie SGB, którego ESBANK jest aktywnym uczestnikiem, to konieczność. Wychodząc z tego założenia, już w 2012 r. udostępniliśmy swoim Klientom własną aplikację mobilną. Jednak żadna technologia nie zastąpi w pełni kontaktu z drugim człowiekiem. I o ile silna ekspansja w zakresie ilości placówek nie ma już w naszym biznesie racji bytu, to dostęp do przyjaznej przestrzeni bankowej i bezpośrednia rozmowa z zaufanym, profesjonalnym doradcą wciąż są potrzebne. Tym potrzebniejsze, im więcej technologii AI nas otacza i szczególnie podczas podejmowania życiowych decyzji finansowych, jak kredyt mieszkaniowy czy wieloletnie zobowiązanie na rozwój firmy.

Nowa lokalizacja w Częstochowie we własnym, a nie wynajmowanym lokalu, wpisuje się w naszą strategię zarządzania zasobami, ale przede wszystkim daje klientom poczucie stabilności, bezpieczeństwa i wsparcia „tuż za rogiem”. To ważny element budowania relacji, które stanowią siłę ESBANKU Banku Spółdzielczego, a zarazem wyróżnik naszego sektora.

I to dawanie klientom poczucia stabilności powoduje, że prowadzicie działalność w 17 lokalizacjach?

Jest to element budowania zaufania do instytucji. Po przejęciu na przełomie 2021 i 2022 roku dawnego BS Kleszczów skupiamy się na wzmacnianiu swojej pozycji w rejonach najbardziej perspektywicznych. Aktualnie działamy na terenie województw łódzkiego i śląskiego, w mniejszych miejscowościach gminnych oraz w miastach jak Radomsko, Częstochowa, Piotrków Trybunalski i Łódź. W tym ostatnim – na razie działa nasze biuro kredytowe, obsługujące firmy i instytucje, bo to segment, w którym budujemy swoją przewagę na mocno konkurencyjnym, łódzkim rynku. Ale już niebawem planujemy przeniesienie tam z podłódzkiego Tuszyna całego oddziału z uniwersalną ofertą produktów bankowych i ubezpieczeniowych.

***O sile banku stanowi przede wszystkim kapitał ludzki, pracownicy, bez których nawet najlepsza wizja rozwoju nie mogłaby być realna.* Wie pan kto to powiedział?**

Nie, natomiast śmiało mógłbym się pod tymi słowami podpisać.

To pan ponad piętnaście lat temu, gdy rozmawialiśmy po raz pierwszy.

Oj, wiele lat minęło. (śmiech) Jesteśmy u progu stulecia ESBANKU Banku Spółdzielczego, który trudne momenty historyczne i gospodarcze przetrwał, stale rosnąc w siłę, właśnie dzięki tworzącym go ludziom. Pracownicy to najcenniejszy zasób każdej firmy i to nie jest frazes. Od zaangażowania, motywacji i profesjonalizmu kadry, od jej wiary we wspólną misję i wartości bezpośrednio zależy realizacja bieżących zadań, które prowadzą nas do wypełnienia celów strategicznych.

W ESBANKU od lat perspektywa personalna jest fundamentem strategii biznesowej banku. Inwestujemy w działania szkolenio-

Najnowsza placówka ESBANKU Banku Spółdzielczego w Częstochowie ulokowana jest w dynamicznie rozwijającej się dzielnicy Parkitka.

we. Rozwijamy programy benefitowe dla pracowników. Dbamy o rozwój komunikacji wewnętrznej, szanując potrzeby informacyjne naszej załogi. Wspieramy też wolontariat pracowniczy, inaugurujemy wspólne działania sportowe i inne aktywności, które integrują nas również po pracy. Chcemy, by nasza kultura organizacyjna wspierała nie tylko zawodowy, ale i osobisty rozwój pracowników ESBANKU, by naprawdę łączyła nas wokół wspólnych idei. To podstawa rozwoju naszej firmy.

Dziś mówi się, że kapitał ma narodowość. Popularne jest hasło, żeby myśleć globalnie, działać lokalnie. Hasło banku brzmi: Jesteśmy dla Ciebie. Co ono oznacza?

Hasło „Jesteśmy dla Ciebie” podkreśla klientocentryczność i siłę relacji. Stanowi też rozwinięcie misji ESBANKU. Nasza deklaracja, że „wspieramy ludzi stąd!” to filozofia wspólnego działania dla dobra lokalnych społeczności. To ta sama idea, którą w Grupie SGB komunikujemy frazą „dobrze dbać o siebie nawzajem”. W ESBANKU z dumą podkreślamy wyłącznie polski kapitał i nierozerwalną więź ze środowiskiem, w którym działamy. Stąd pochodzimy, tu mieszkamy, tutaj też po sąsiedzku udostępniamy usługi finansowe, które nie odbiegają od standardów banków komercyjnych. Tu od blisko 100 lat budujemy kapitał i także tutaj dzielimy się częścią wypracowanych zysków. Wspierając marzenia i cele naszych klientów, angażując się w oddolne inicjatywy, które aktywizują i integrują lokalne społeczności, a także inicjując pozytywne zmiany w najbliższym otoczeniu – przyczyniamy się do społecznego i gospodarczego rozwoju naszych małych ojczyzn.

Polska otrzymała pierwszą transzę środków z KPO. Czy klienci i bank mogą na tym skorzystać?

W ESBANKU mamy doświadczenie w pozyskiwaniu środków unijnych na działania szkoleniowe. Wspomnę choćby projekt Bankowa Akademia Rozwoju i ponad 680 tys. zł dotacji na rozwój wiedzy i kompetencji naszych kadr w latach 2014-2015. Śledzimy sytuację i chętnie skorzystamy z nowych możliwości. Na pewno, tak jak dotychczas, będziemy włączać się – dzięki współpracy SGB-Banku i BGK – w dystrybucję instrumentów finansowanych ze środków Unii Europejskiej, takich jak gwarancje i poręczenia. Unijne wsparcie w zakresie tańszych, łatwiej dostępnych kredytów dla przedsiębiorców to szansa dla wielu lokalnych firm na rozwój biznesu czy jego zieloną transformację. Chcemy być częścią takich programów pomocowych.

SGB oferuje swoim klientom nowoczesne produkty. Aplikacje mobilne, Kantor SGB, przelewy BLIK. Te usługi ma w ofercie także ESBANK. Czy to przewaga konkurencyjna?

Bank, jakiego potrzebuje współczesny klient, to od dawna już nie tylko konto, kredyt i lokata. Nawet bankowość internetowa to za mało, bo liczy się możliwie kompleksowy dostęp do usług banku na wyciągnięcie ręki ze smartfonem. Bez nowoczesnej, mobilnej oferty nie moglibyśmy konkurować z komercyjnymi gigantami. Tymczasem, także dzięki współpracy z SGB-Bankiem w ramach Systemu Usług SGB, nasz katalog zdalnych usług nie ustępuje największym bankom. Łamiemy stereotypy dotyczące

Jednak żadna technologia nie zastąpi w pełni kontaktu z drugim człowiekiem.

bankowości spółdzielczej i bez kompleksów łączymy bankowość opartą o relacje – czyli coś, co wyróżnia bankowość spółdzielczą – z nowymi, bankowymi technologiami. I choć cały czas mamy nad czym pracować, to nasi klienci ten stały rozwój doceniają.

Dziś, żeby utrzymać się na rynku, trzeba stosować cross-selling. Aby zwiększyć sprzedaż w SGB proponowany jest Nowy Model Sprzedaży. Co pan myśli o tym projekcie?

Doceniam wszelkie działania Banku Zrzeszającego, które podnoszą jakość usług w naszej Grupie, bo w ten sposób wspólnie wzmacniamy pozytywny wizerunek sektora banków spółdziel-

FOT. ARLETA WĘGRZYŃSKA ESBANK BS

czych. W ESBANKU już w 2010 roku wdrożyliśmy standardy obsługi, obejmujące zasady efektywnej sprzedaży oraz budowania pozytywnego doświadczenia klienta. To know-how stale rozwijamy. Dostosowujemy je do zmieniających się potrzeb klientów oraz naszych możliwości w zakresie produktów i usług. Aktywne badanie potrzeb klienta czy wspomniany cross-selling to podstawa pracy naszych doradców, np. w zakresie łączenia produktów i usług bankowych oraz ubezpieczeniowych.

Na czym jeszcze opiera się marketing usług i produktów ESBANKU?

ESBANK jest uniwersalną instytucją finansową. Obsługujemy zarówno klientów indywidualnych, jak i rolników, firmy, instytucje oraz samorządy, przy czym specjalizujemy się w finansowaniu klientów z sektora MŚP. Chcemy odpowiadać na aktualne potrzeby różnych grup odbiorców naszej oferty. Stąd wspomniane już, często pionierskie w Grupie SGB, testowanie i wdrażanie w ramach SUS nowości produktowych oraz technologicznych, których implementacja jest dla nas dużo łatwiejsza dzięki kapitałowej i organizacyjnej sile Zrzeszenia.

Jesteście też multiagentem ubezpieczeniowym. Na czym to polega?

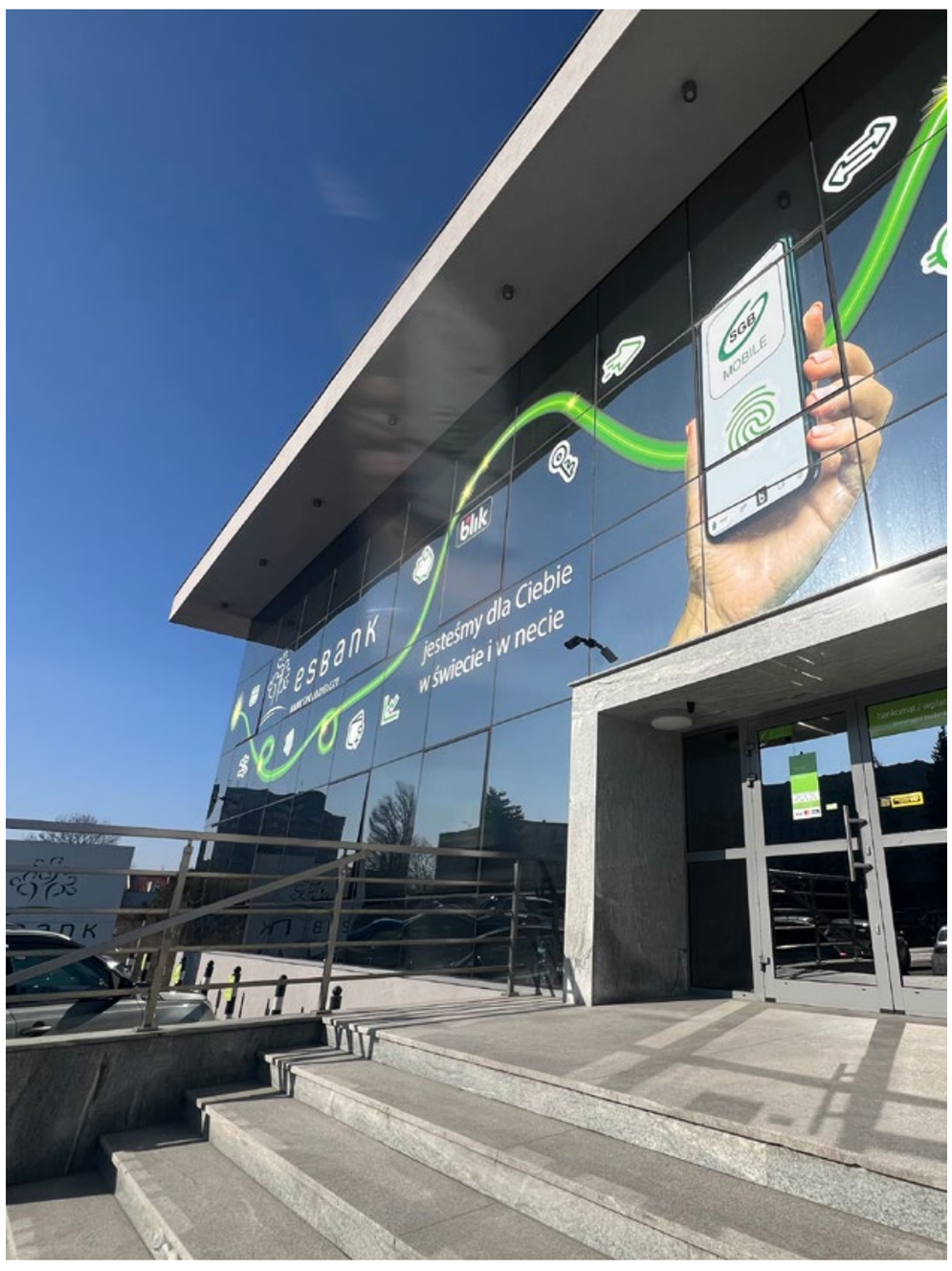
Naszym własnym pomysłem jest wzmocnienie działalności banku jako multiagenta. Aktualnie współpracujemy z 16 renomowanymi towarzystwami ubezpieczeniowymi. Rozwijana od wielu lat, kompleksowa oferta ubezpieczeniowa dla klientów indywidualnych, firm i samorządów uzupełnia pakiet klasycznych usług finansowych, dostępnych w każdej placówce ESBANKU. Ubezpieczamy zdrowie, życie i mienie, nasza oferta obejmuje zarówno proste polisy komunikacyjne, jak i ubezpieczenia ryzyk budowlano-montażowych czy gwarancje ubezpieczeniowe dla przedsiębiorców. Zapewniamy też klientom pomoc na każdym etapie obsługi posprzedażowej oraz likwidacji szkód.

Z roku na rok ten obszar stanowi coraz ważniejszą pozycję w strukturze naszych przychodów. Dlatego też z końcem 2023 roku powołaliśmy do życia submarkę ESBANK Ubezpieczenia, która wraz z hasłem uzupełniającym #DobrzeUbezpieczamy na stałe wpisuje się już w nasze działania marketingowe. Nowe logo pojawia się w kolejnych bankowych przestrzeniach, podkreślając wizualnie komplementarność naszej oferty.

W ESBANKU z dumą podkreślamy wyłącznie polski kapitał i nierozerwalną więź ze środowiskiem, w którym działamy.

Czy audytorzy już zweryfikowali wyniki finansowe banku za 2023 rok? Jak pan je podsumuje? Jaki to był rok?

W marcu, kiedy rozmawiamy, jesteśmy jeszcze w trakcie niezależnego audytu finansowego. Mamy za sobą rok, który był rekordowy pod względem osiąganych przez bank wyników, a jednocześnie był kolejnym okresem dużej niestabilności i niepewności w otoczeniu makroekonomicznym. Udało nam się odpowiednio wykorzystać otoczenie stóp procentowych oraz efektywnie zarządzać ponoszonymi kosztami. Dzięki temu wypracowany zysk brutto za 2023 rok przekroczył 30 mln zł i był większy o ponad 6 mln zł od uzyskanego w 2022 roku. Wskazuje to słuszność kierunków obranych w perspektywie strategicznej na lata 2022-2024.



Hasło „Jesteśmy dla Ciebie” podkreśla klientocentryczność i siłę relacji. Stanowi też rozwinięcie misji ESBANKU. W ESBANKU z dumą podkreślamy wyłącznie polski kapitał i nierozerwalną więź ze środowiskiem, w którym działamy.

Na bardzo konkurencyjnym rynku usług finansowych trzeba umieć dotrzeć do młodych klientów. Jaki pomysł na pozyskanie młodego klienta ma ESBANK?

To poważne wyzwanie. Ważnym krokiem w realizacji tego strategicznego celu było wdrożenie BLIKA na telefon w naszej aplikacji mobilnej. Szansą jest też nowa wersja aplikacji SGB Mobile Junior, która wesprze nas w przyciągnięciu i przywiązaniu do banku dzieci naszych klientów. Poza nowoczesną ofertą, dostępną w lokalnym banku, wzmacniamy działania w obszarze CSR, kierowane do młodych mieszkańców terenu naszego działania. Współpraca ze szkołami w obszarze edukacji oraz sponsoring inicjatyw skierowanych do młodzieży pomaga nam budować rozpoznawalność i pozytywne skojarzenia z marką. Czy to wszystko zaowocuje pierwszym kontem i pierwszym kredytem właśnie u nas – pokaże czas.

Młody klient oczekuje innej bankowości.

Tak. On na pewno do placówek bankowych nie przychodzi… ale z czasem staje się starszy, zmieniają się jego priorytety. Wtedy przyjdzie do nas na przykład po kredyt hipoteczny. Wówczas zwiąże się z nami na wiele lat. A jeśli nasza oferta – zwłaszcza ta wspólna, zrzeszeniowa – będzie nadążać za trendami i zaspokoi podstawowe potrzeby bankowe młodego człowieka, dziś założy u nas konto na selfie – a jutro doceni nasze personalne podejście do klienta.

Innym równie ważnym wyzwaniem w sektorze jest cyberbezpieczeństwo. Jak ważny jest to obszar dla banku? Czy popularyzujecie edukację wśród klientów? Z badań wynika, że najczęściej klienci padają ofiarą przestępstw przez swoją nieuwagę.

Od lat aktywnie edukujemy klientów i lokalną społeczność w zakresie cyberbezpieczeństwa i bezpiecznego bankowania. Cykle edukacyjne ESBANK radzi czy CYBERczwartek z ESBANKIEM, obok bieżących komunikatów bezpieczeństwa na

FOT. ARLETA WĘGRZYŃSKA ESBANK BS

stałe wpisały się już w naszą komunikację w lokalnych mediach, social mediach banku i biuletynie firmowym „ESBANK z bliska”, uzupełniając bezpośredni kontakt z klientami w placówkach. Zwiększanie świadomości użytkowników bankowości elektronicznej musi oczywiście iść w parze ze stałym wzmacnianiem systemów bezpieczeństwa i antyfraudowych w ramach bankowej infrastruktury teleinformatycznej. Takie też są nasze priorytety.

Żyjemy w niespokojnych czasach, patrząc w skali makro i mikro. Jakie widzi pan perspektywy? Jak widzi pan przyszłość sektora bankowości spółdzielczej?

Musimy wytrwale robić swoje. Z tradycją w sercu, ale z głową otwartą na wyzwania przyszłości. Naszą szansą jest współpraca w ramach Zrzeszenia i unifikacja działań tam, gdzie to możliwe, ale z poszanowaniem różnorodności poszczególnych Banków Spółdzielczych SGB, ich specyfiki i indywidualnej sytuacji. Wierzę w przewagę, jaką niesie ze sobą bankowość relacyjna, która wykorzystuje, ale nie daje się wyprzeć nowoczesnej technologii.

Nie sądzi pan, że algorytmy dopasują produkty do klientów?

Nie do końca. Bezduszne algorytmy wciąż jeszcze się mylą. Poza tym u konkurencji zawsze będą schematy, do których klient – jego dochody, okres kredytowania, cel inwestycji – będą tylko pozycją w tabeli, wpisaną w szablon. Jeśli klient wyjdzie poza ramę, nie dostanie wsparcia.

Bez nowoczesnej, mobilnej oferty nie moglibyśmy konkurować z komercyjnymi gigantami.

Przykład?

Jeden z klientów chciał kupić dwa mieszkania w Warszawie i połączyć je w jedno. W bankach, w których się pojawił, nie dostał kredytu. Jak to: jeden kredyt na dwa mieszkania? U nas sprawę załatwił. Byliśmy elastyczni. To jest przewaga bankowości spółdzielczej. Dlatego musimy być w stałej gotowości, by jak dotąd szybko i efektywnie reagować na wyzwania współczesnego świata, dając naszym klientom stabilny dostęp do pieniędzy.

Skoro sektor jest tak dobry, to dlaczego nie ma tak dużych udziałów w rynku?

Jesteśmy bankowością lokalną. Na przykład w powiatach nasz udział w rynku, w zależności od portfela, sięga 30%. To specyfika lokalności. Inaczej to wygląda w globalnych liczbach, ale trudno, żeby bankowość spółdzielcza finansowała międzynarodowe korporacje.

A konsorcja finansowe?

To dobry pomysł Banku Zrzeszającego. One nam bardzo dobrze wychodzą na przykład w przypadku obsługi budżetów sejmików wojewódzkich. Wiele rzeczy nam dobrze wychodzi, ale jeśli chcemy więcej znaczyć – powinniśmy oferować najlepsze produkty i rozwijać to, w czym jesteśmy najlepsi, czyli relacyjność i lokalność. ●

Radomsko, 12 marca 2024 r.

Rozmawiali: Arleta Węgrzyńska, Roman Szewczyk

Siedziba banku mieści się w nowoczesnym budynku w centrum Radomska. Obiekt wyposażony jest w rozwiązania ekologiczne, m.in. fotowoltaikę i przyciąga uwagę także nocą.

FOT. ARLETA WĘGRZYŃSKA ESBANK BS

Usługi cyberbezpieczeństwa

dla Banków Spółdzielczych SGB

Daniel Krzywiec
SGB-Bank SA

Motorem naszych działań jest bezpieczeństwo klientów Zrzeszenia SGB i satysfakcja banków spółdzielczych. Wyróżnia nas kompleksowe podejście do kwestii cyberbezpieczeństwa podczas projektowania i wdrażania usług dla banków spółdzielczych. W ramach każdej usługi biznesowej, bank spółdzielczy otrzymuje w standardzie pełen pakiet jej ochrony. Inwestujemy bardzo duże środki w mechanizmy bezpieczeństwa, wdrażając najnowocześniejsze rozwiązania technologiczne oparte na innowacyjnych produktach i usługach.

Zbudowaliśmy Centrum Kompetencyjne SGB

skupiające dedykowaną grupę specjalistów, których misją jest zapewnienie bankom spółdzielczym dostępu do pożądanych, lecz często deficytowych funkcji, kompetencji i umiejętności w obszarze cyberbezpieczeństwa. Doskonale rozumiemy, że obszar cyberbezpieczeństwa to istotna część biznesu, która musi być oparta na silnym i kompetentnym zespole. Nieustannie podnosimy swoje kwalifikacje poprzez uczestnictwo w specjalistycznych szkoleniach i zdobywaniu certyfikatów branżowych.

Centrum Operacji Bezpieczeństwa SGB wykorzystuje nowoczesne technologie, procedury bezpieczeństwa oraz pracę ludzi odpowiedzialnych za szybkie wykrywanie i analizę zagrożeń dla usług świadczonych w ramach Zrzeszenia SGB.

Banki spółdzielcze korzystające z usług SGB-Banku SA mają dostęp do najnowocześniejszej technologii, kompetencji eksperckich oraz współpracują z liderami rynku w obszarze cyberbezpieczeństwa. Usługi cyberbezpieczeństwa SGB są przedmiotem systematycznych, niezależnych audytów oraz podlegają nadzorowi przez Urząd Komisji Nadzoru Finansowego i System Ochrony Instytucjonalnej. Wszystko to sprawia, że jesteśmy rzetelnym i zaufanym partnerem dla banków spółdzielczych.
W ramach świadczonych usług banki spółdzielcze otrzymują m.in.:

Security Operations Center

Centrum Operacji Bezpieczeństwa SGB dla banków spółdzielczych wykorzystuje nowoczesne technologie, procedury bezpieczeństwa oraz pracę ludzi odpowiedzialnych za szybkie wykrywanie i analizę zagrożeń dla usług świadczonych w ramach Zrzeszenia SGB. Do podstawowego zakresu obowiązków SOC należy m.in.:

- analiza i korelacja zdarzeń bezpieczeństwa,
- dostarczanie wskaźników IoC (ang. Indicator of Compromise) dla istotnych zagrożeń sektorowych,
- monitorowanie i ochronę ruchu sieciowego,
- Web Filtering i detekcja złośliwego kodu na styku sieci internet,
- zarządzanie podatnościami technicznymi oraz przeprowadzanie testów penetracyjnych,
- koordynacja incydentów cyberbezpieczeństwa na poziomie sektora finansowego,
- monitorowanie działań użytkowników uprzywilejowanych,
- monitorowanie zdalnych sesji dostępu do infrastruktury teleinformatycznej banku,
- monitorowanie integralności plików.

Sztuczna inteligencja

Aby zwiększyć skuteczność i wydajność operacyjnego centrum bezpieczeństwa SGB, wdrożyliśmy platformę wykrywania i reagowania na zdarzenia sieciowe opartą na technologii sztucznej inteligencji. Sztuczna inteligencja prowadzi analizę ruchu siecio-

wego w celu zidentyfikowania wzorców wykraczających poza normę. Rozwiązanie wykorzystuje połączenie uczenia nadzorowanego i nienadzorowanego w celu wykrywania zachowań atakujących i użytkowników końcowych oraz naśladowania i przewidywania ich działań. Jej działania nadają priorytet alertom i inicjują właściwą odpowiedź, wspierając pracę analityków bezpieczeństwa SGB.

Bezpieczeństwo usług bankowości internetowej i mobilnej

Bezpieczeństwo jest dla nas podstawowym warunkiem rozwoju usług bankowości internetowej i mobilnej. Wdrożone rozwiązania umożliwiają wykrywanie anomalii na rachunku klienta, blokowanie kanałów dostępu oraz zrywanie podejrzanych sesji. W ramach usługi możliwe jest aktywne i szybkie reagowanie na pojawiające się nowe metody działania oszustów oraz odpowiadanie na najczęściej realizowane przez przestępców scenariusze wyłudzeń danych i kradzieże środków. Wykorzystujemy zaawansowaną analitykę bazującą na profilach klientów, urządzeń i lokalizacji. Przetwarzamy dane z wielu systemów bankowych, które następnie procesowane są w silniku analitycznym, co umożliwia wykrycie podejrzanych aktywności i transakcji w czasie rzeczywistym.

SGB-Bank SA odpowiedzialny jest za:

- rozwój i utrzymanie platformy wykrywania nadużyć,
- projektowanie i wdrażanie mechanizmów detekcyjnych i prewencyjnych (wykrywanie podejrzanej aktywności i zapobieganie oszustwom),
- wdrażanie procedur i obsługę zdarzeń bezpieczeństwa (analizę, wyjaśnianie zdarzeń, kierowanie ostrzeżeń do klientów),
- wsparcie oraz koordynowanie współpracy z Policją, Prokuraturą, Centralnym Biurem Zwalczania Cyberprzestępczości, CSIRT KNF, CERT NASK, CSIRT GOV, FINCERT Bankowego Centrum Cyberbezpieczeństwa ZBP, instytucjami finansowymi, operatorami telekomunikacyjnymi,
- obsługę komunikacji z klientami banków spółdzielczych w celu potwierdzenia transakcji i blokowania środków dostępu (Call Center 24h).

Ponadto do dyspozycji banków spółdzielczych uruchomiona została 24h Infolinia CYBER SGB.

Skuteczność usługi FDS jest bardzo wysoka, co potwierdzają dane za 2023 r., gdzie udział procentowy wartości transakcji oszukańczych w bankach spółdzielczych SUS stanowił 0,23% do wartości transakcji oszukańczych całego sektora finansowego w Polsce.

Cyber Threat Intelligence (CTI)

Usługa CTI to stałe pozyskiwanie i dostarczanie informacji z zewnętrznych źródeł dotyczących cyberzagrożeń. Zakres usługi obejmuje bieżący monitoring i analizę wielu źródeł informacji o cyberzagrożeniach, które mogą mieć wpływ na integralność i dostępność systemów banków spółdzielczych oraz ich klientów. Dostarczane dane stanowią istotny element procesu ochrony przed nowymi i celowanymi atakami tworząc kolejną linię wsparcia dla Security Operation Center oraz istotne źródło danych zewnętrznych automatycznie zasilających systemy ochrony bezpieczeństwa sieci.

W ramach usługi CTI, SGB-Bank SA dostarcza bankom spółdzielczym m.in.:

- wsparcie w reagowaniu i obsłudze incydentów,
- aktywne monitorowanie źródeł nieindeksowanych warstw internetu w poszukiwaniu istotnych informacji mogących mieć wpływ na bezpieczeństwo banków spółdzielczych,
- dostarczanie informacji o obserwowanych zagrożeniach (alerty SGB, dwutygodniowy biuletyn CTI tj. przegląd cyberzagrożeń nt. kampanii phishingowych, trojanów bankowych, ransomware, fałszywych aplikacji w sklepach GooglePlay i App Store, zmian prawnych w obszarze cyberataków i wycieków danych na świecie, raporty dot. nowych podatności),
- monitorowanie działań środowisk naruszających bezpieczeństwo,
- monitorowanie wycieków danych,
- informacje o kontach słupów i fałszywych „bramkach płatniczych".

Ochrona DDoS

Ataki DDoS są ukierunkowane na witryny internetowe, serwery czy aplikacje bankowe. Co istotne, atak ten jest przeprowadzany przy wykorzystaniu wielu urządzeń zainfekowanych złośliwym oprogramowaniem, kontrolowanych przez cyberprzestępców. Ze względu na duże rozproszenie ataku, jego zatrzymanie i zidentyfikowanie sprawców jest niezwykle trudne. Ochrona DDoS usług SGB polega na monitorowaniu ruchu sieciowego i wykrywaniu anomalii (mogących skutkować wysyceniem łącza i utratą ciągłości procesów biznesowych) oraz eliminacji podejrzanych pakietów. Banki Spółdzielcze SGB otrzymują gwarancję natychmiastowej reakcji na atak oraz znaczne ograniczenie ryzyka utraty ciągłości działania kluczowych procesów. To z kolei przekłada się na wizerunek oraz ograniczenie ryzyka niedostępności usług bankowości elektronicznej. ●

Bezpieczeństwo jest dla nas podstawowym warunkiem rozwoju usług bankowości internetowej i mobilnej.

Uruchomiliśmy nową usługę monitoringu transakcji kartowych dla Banków Spółdzielczych SGB. Nowe podejście do sposobu analizy zachowań transakcyjnych klienta, polega na weryfikowaniu kartowego profilu transakcyjnego klienta i wykrywaniu anomalii transakcyjnych. W ramach usługi zautomatyzowaliśmy cały proces obsługi alertów.

KLIKNIJ ŻEBY POSŁUCHAĆ ARTYKUŁU

Phishing w erze AI:

jak chronić się przed oszustami, którzy wiedzą, jak korzystać ze sztucznej inteligencji?

Krzysztof Swoboda
Technical Content Manager w Takaoto.pro

Sztuczna inteligencja jest tu i teraz. Ze wszystkimi swoimi zaletami, ale i wieloma zagrożeniami, które zmuszą nas do przemodelowania naszego trybu życia. Jednym z obszarów ryzyka jest phishing. To od dawna znana taktyka wyłudzania danych, która dzięki AI znów stanowi spore zagrożenie. internet Crime Complaint Center alarmuje, że tylko w Stanach Zjednoczonych rokrocznie dochodzi do ponad 300 tysięcy udanych ataków opierających się na phishingu. Jak bronić się przed cyberprzestępcami, którzy korzystają z oprogramowania bazującego na sztucznej inteligencji?

Scam, phishing i rozbudowane, wielopoziomowe kradzieże danych dzięki AI?

Rozwój sztucznej inteligencji otworzył drzwi do nowych cyberprzestępstw, które są niezwykle trudne do wykrycia i zneutralizowania. Hakerzy korzystają z zaawansowanych algorytmów, aby analizować ogromne zbiory danych. Identyfikują potencjalne cele i dostosowują swoje metody ataku do wybranych osób.
W przeciwieństwie do słynnych maili od nigeryjskiego księcia (które otrzymywali praktycznie wszyscy, bez względu na wiek, płeć czy miejsce zamieszkania), nowoczesne narzędzia bazujące na AI potrafią tworzyć profile szczególnie zagrożonych grup docelowych, a następnie wyszukiwać takie osoby. Mogą to być np. seniorzy, osoby szukające partnerów na portalach randkowych czy dzieci dobrze sytuowanej klasy średniej.

Eksperci są zgodni: kluczem jest ciągła edukacja. Nie musisz zapisywać się na specjalistyczne kursy, jednak warto być na bieżąco: przeglądać ogólnopolskie portale informacyjne i nie bagatelizować potencjalnych zagrożeń.

Własne modele sztucznej inteligencji mogą tworzyć praktycznie wszyscy – także cyberprzestępcy. I bardzo chętnie korzystają z tej możliwości.

Wiemy o co najmniej kilku autorskich modelach sztucznej inteligencji, które stworzyli cyberprzestępcy. Te najpopularniejsze to Freud oraz WormGPT. Bazują one na ogólnodostępnych wersjach sztucznej inteligencji, które następnie są rozwijane w taki sposób, by z ich pomocą można było:

- gromadzić dane,
- przeszukiwać pliki graficzne, np. zdjęcia kart kredytowych z widocznym kodem CVV,
- tworzyć spreparowane wiadomości e-mail, które – zdaniem specjalistów z branży Cyber Security oraz Interpolu – są niezwykle trudne do odróżnienia od korespondencji, jaką napisałby człowiek.

Sztuczna inteligencja próbuje okraść nas na kilku różnych poziomach

Wielopoziomowa kradzież danych może bazować na kilku różnych schematach. Najczęściej cyberprzestępcy próbują zdobyć nasze zaufanie, a więc wybierają długi, angażujący proces. Dlaczego? Ponieważ wtedy można zebrać wiele cennych danych zarówno o ofierze, jak i o jej bliskich.
Wyobraź sobie, że do starszej osoby, która nie jest świadoma cyfrowych zagrożeń, generatywna sztuczna inteligencja pisze od razu: „Cześć, jestem amerykańskim żołnierzem, utknąłem w Afganistanie. Wyślij mi 1000 dolarów, bo nie mam jak wrócić do domu, a w zamian, po powrocie, oddam Ci 1500 USD”.

To nie zadziała. To proste, budowane na jednej płaszczyźnie oszustwo, które niewiele różni się od oszustw „na spadek” od wujka mieszkającego w Nigerii czy od tajemniczego krewniaka, od którego mamy odebrać wart miliony obraz – jeśli tylko wcześniej zapłacimy w kryptowalutach ułamek jego wartości. Dzięki mediom mainstreamowym oraz wielu kampaniom społecznym nauczyliśmy się dość dobrze rozpoznawać te zagrożenia.

Inżynieria społeczna wspomagana przez sztuczną inteligencję staje się wyjątkowo skutecznym narzędziem w rękach przestępców. Wykorzystując AI, cyberprzestępcy są w stanie budować głębokie relacje ze swoimi ofiarami, przełamując naturalne mechanizmy obronne, które ludzkość wykształciła w toku ewolucji. Nasze zabezpieczenia psychologiczne często zawodzą w obliczu intensywnych emocji, takich jak miłość, stres czy wizja zdobycia upragnionych dóbr. Dzięki AI

A czy jest się czego bać? Wciąż słyszymy o kreatywnych formach kradzieży: na wnuczka, na zapomnianego krewniaka czy na aktora lub żołnierza, który dziwnym trafem może poprosić o pomoc właśnie Ciebie.

manipulacja staje się jeszcze bardziej wyrafinowana i dociera do głęboko ukrytych pragnień i lęków. To właśnie dlatego połączenie sztucznej inteligencji z inżynierią społeczną jest tak wielkim zagrożeniem.

Posługując się przykładem amerykańskiego żołnierza, sztuczna inteligencja wygeneruje taką osobę i stworzy jej cyfrowy głos, który dzięki technologii deep fake będzie brzmiał bardzo naturalnie. Ofiara zobaczy tę postać, usłyszy ją, pozna jej historię, a być może nawet się w niej zakocha. Dzięki kilku sztuczkom psychologicznym będzie uzależniona emocjonalnie od kogoś, kto tak naprawdę nie istnieje.

Model zbierze szereg danych behawioralnych, a jeśli rozmówca wyśle swoją fotografię, to zostanie ona rozpracowana na szczegóły. Może w tle, na zdjęciach, widać osoby z rodziny? A może uda się zeskanować wzór linii papilarnych, jeśli rozmówca na nagraniu wideo pokaże otwartą dłoń do kamery? Tak cennych danych specjaliści, dodatkowo wspierani przez AI, z pewnością nie pominą.

Gdy czytasz w sieci o tym, że ktoś przelał oszczędności życia nieistniejącemu amerykańskiemu żołnierzowi, by ten mógł wrócić do domu, musisz zdać sobie sprawę z tego, że specjaliści i algorytmy AI mogły pracować nad taką osobą przez kilka tygodni, nierzadko miesięcy. To ta ciemniejsza, mroczna strona sztucznej inteligencji, o której zawsze należy pamiętać.

Strategie ochrony, czyli jak bronić się przed AI?

Eksperci są zgodni: kluczem jest ciągła edukacja. Nie musisz zapisywać się na specjalistyczne kursy, jednak warto być na bieżąco: przeglądać ogólnopolskie portale informacyjne i nie bagatelizować potencjalnych zagrożeń, o których piszą takie serwisy jak Niebezpiecznik. Z pewnością nie wolno bagatelizować tych zagrożeń – portal analityczny Statista szacuje, że w Polsce rokrocznie dochodzi do co najmniej 15 tysięcy przestępstw bankowych opierających się na phishingu.

Ofiarami ataków cyberprzestępców zwykle padają ci, którzy twierdzili, że są zbyt inteligentni, by oszukała ich maszyna.

Bezpieczeństwo w sieci to także jeden z ważniejszych obszarów tzw. społecznej odpowiedzialności biznesu. Na szczęście coraz więcej firm zdaje sobie z tego sprawę i wdraża np. dodatkowe zabezpieczenia dla aplikacji bankowych czy systemów uwierzytelniania użytkownika.

Zauważyłeś, że od pewnego czasu, gdy chcesz szybko autoryzować swoje konto, nie wystarczy już skan lub zdjęcie dowodu osobistego? Obecnie kluczowy nacisk kładzie się na tworzenie prostych modeli 3D twarzy użytkownika: musisz aktywować aplikację, a następnie, w czasie rzeczywistym, poruszyć głową od lewej do prawej.

To rozwiązanie, które ma przekonać algorytm, że po drugiej stronie znajduje się świadoma swojej decyzji osoba, która faktycznie chce założyć konto w banku lub autoryzować przewalutowanie środków. Co warto podkreślić, takie rozwiązanie działa w wielu różnych segmentach rynku:

- w instytucjach finansowych,
- na wybranych giełdach kryptowalut,
- w najlepszych niepublicznych zakładach opieki zdrowotnej,
- w firmach bukmacherskich.

Bez międzysektorowej współpracy i stworzenia jednolitych standardów, przewagę zyskają cyberprzestępcy. Jeśli jednak strona rządowa i świat biznesu dojdą do porozumienia i wypracują nowe metody ochrony i monitorowania sieci, to są spore szanse na to, że nawet najdoskonalszy phishing bazujący na sztucznej inteligencji przestanie być tak dużym zagrożeniem jak obecnie.

A czy jest się czego bać? Wciąż słyszymy o kreatywnych formach kradzieży: na wnuczka, na zapomnianego krewniaka czy na aktora lub żołnierza, który dziwnym trafem może poprosić o pomoc właśnie Ciebie, a nie ambasadę czy swojego agenta. Odpowiedź nasuwa się sama. ●

Bezpieczne bankowanie

Nie daj się oszustom! Zapoznaj się z metodami, które najczęściej stosują

PHISHING

to metoda oszustwa, która polega na wysyłaniu e-maili lub SMS-ów z załącznikami czy linkami do fałszywych stron internetowych. Fałszywe wiadomości najczęściej dotyczą niewielkiej kwoty, którą masz dopłacić do przesyłki albo rzekomo niezapłaconej faktury, którą masz natychmiast opłacić. Mogą też dotyczyć rzekomych problemów z Twoim kontem lub płatnością.

VISHING I SPOOFING

Vishing to metoda oszustwa polegająca na podszywaniu się pod pracowników banków i innych zaufanych instytucji np. policjantów. Oszuści chcą w ten sposób zdobyć Twoje poufne dane (np. login i hasło do bankowego konta internetowego). Mogą Cię też nakłaniać do instalacji podejrzanej aplikacji do zdalnej obsługi urządzenia. Spoofing to z kolei metoda oszustwa polegająca na podszywaniu się pod inne urządzenia lub innego użytkownika. Oszuści zmieniają numer telefonu, adres e-mail czy adres IP, z których się kontaktują. Zawsze są znakomicie przygotowani do rozmowy.

FAŁSZYWE INWESTYCJE

to metoda oszustwa polegająca na podszywaniu się pod maklerów i brokerów giełdowych. Proponują nowe możliwości zainwestowania Twoich środków, które np. wcześniej nie były dostępne na rynku dla każdego. Doskonale przedstawiona oferta staje się przekonująca, przez co ciężko rozpoznać kłamstwo. Co więcej, oszuści bardzo często wykorzystują wizerunki znanych osób czy firm. Dzięki temu oferta i możliwość szybkiego oraz wysokiego zarobku wydają się jeszcze bardziej wiarygodne.

Jak się chronić przed tymi wszystkimi oszustami?

- Zanim klikniesz w link lub pobierzesz jakiś plik, upewnij się, że pochodzą one z zaufanych źródeł.
- Filtruj spam i zainwestuj w oprogramowanie antywirusowe, najlepiej z modułem antyphishingowym.
- Nie podawaj loginu i hasła do bankowości internetowej oraz danych karty płatniczej (numer karty, CVV, data ważności).
- Jeżeli jakakolwiek rozmowa wzbudza Twoje wątpliwości lub niepokój, rozłącz się. Chwilę później samodzielnie połącz się z instytucją, z której dzwonił rzekomy przedstawiciel. Koniecznie wpisz numer samodzielnie, nie oddzwaniaj na wcześniejsze połączenie.
- Nigdy nie instaluj dodatkowego oprogramowania na urządzeniach, za pomocą których logujesz się do aplikacji bankowej.
- Omijaj podejrzane inwestycje. Zawsze przemyśl wszystkie za i przeciw.
- Jeśli masz podejrzenie, że to oszustwo, zadzwoń na policję.

Bezpieczny internet SGB

Usługi IT dla Banków Spółdzielczych SGB

Piotr Mazur
SGB-Bank SA

W dobie cyfrowej transformacji

sektor bankowości spółdzielczej w Polsce stoi przed wyzwaniem zapewnienia bezpiecznego dostępu do internetu dla swoich pracowników i systemów. W kontekście rosnącej liczby zaawansowanych cyberzagrożeń, ochrona infrastruktury IT oraz danych klientów staje się priorytetem nie tylko ze względów operacyjnych, ale przede wszystkim w trosce o utrzymanie zaufania i reputacji. W niniejszym artykule przyjrzymy się kluczowym aspektom i najlepszym praktykom związanym z bezpieczeństwem dostępu do sieci w bankach, analizując zarówno wyzwania, jak i możliwości, które niesie ze sobą cyfrowa era. Omówimy, w jaki sposób instytucje te mogą skutecznie zarządzać ryzykiem cybernetycznym. Pokażemy usługi, które oferuje bankom spółdzielczym SGB-Bank jako bank zrzeszający, a mogące w znaczny sposób mitygować te ryzyka. W obliczu ciągle zmieniającego się krajobrazu zagrożeń, banki spółdzielcze muszą nieustannie adaptować swoje strategie cyberbezpieczeństwa, aby zapewnić, że dostęp do internetu pozostaje bezpieczny, efektywny i zgodny z obowiązującymi regulacjami.

Używanie internetu i poczty e-mail przez pracowników banków spółdzielczych niesie ze sobą szereg potencjalnych zagrożeń, które mogą zagrozić bezpieczeństwu danych klientów oraz integralności systemów bankowych. Obejmują one:

- Phishing i inne rodzaje oszustw e-mailowych. Pracownicy mogą stać się celami ataków phishingowych, które mają na celu wyłudzenie poufnych danych, takich jak dane logowania lub informacje o klientach.
- Malware i ransomware. Pliki pobrane z internetu lub załączniki e-mail mogą zawierać złośliwe oprogramowanie, które zainfekuje systemy bankowe, prowadząc do utraty danych, zakłóceń w działaniu lub nawet wymuszania okupu za odblokowanie zaszyfrowanych danych.
- Wyciek danych. Nieostrożne korzystanie z internetu i poczty e-mail może doprowadzić do przypadkowego wycieku wrażliwych informacji, co narusza przepisy o ochronie danych osobowych i może prowadzić do poważnych konsekwencji prawnych oraz utraty zaufania klientów.

Znaczenie bezpiecznego dostępu do sieci internetowej

ze stacji roboczych w banku spółdzielczym jest nie do przecenienia. Obejmuje to zastosowanie zaawansowanych rozwiązań bezpieczeństwa, takich jak silne szyfrowanie, bezpieczne połączenia VPN, systemy wykrywania i zapobiegania intruzom (IDS/IPS), zaawansowane narzędzia antywirusowe i antyphishingowe, a także skonfigurowanie zapór ogniowych do monitorowania i kontrolowania ruchu sieciowego. Będziemy również potrzebować zespołu SOC (Security Operations Center), którego głównym zadaniem jest zapewnienie ciągłego monitorowania i analizy bezpieczeństwa systemów informatycznych banku w czasie rzeczywistym, aby szybko wykrywać, reagować i zapobiegać incydentom bezpieczeństwa cybernetycznego.

Zapewnienie bezpiecznego dostępu do internetu i poczty e-mail w banku spółdzielczym jest fundamentalne dla ochrony przed cyberzagrożeniami.

Biorąc pod uwagę skalę działania banków spółdzielczych, kluczowe staje się efektywne zarządzanie zasobami i priorytetyzacja inwestycji w cyberbezpieczeństwo. Banki muszą skupić się na najbardziej krytycznych aspektach swojej infrastruktury IT, jednocześnie wykorzystując dostępne narzędzia i technologie w celu optymalizacji kosztów. Możliwym rozwiązaniem jest również szukanie synergii poprzez współpracę z bankiem zrzeszającym w zakresie wspólnych inicjatyw bezpieczeństwa.

Usługi dla Banków Spółdzielczych SGB

SGB-Bank SA oferuje zestaw usług związanych z podniesieniem poziomu cyberbezpieczeństwa w zrzeszonych bankach spółdzielczych:

- Zarządzanie Siecią WAN – Nasze sieci zbudowane są w oparciu o bezpieczną technologię MPLS. Redundancja połączeń realizowana jest za pomocą bezprzewodowej łączności LTE. Dywersyfikacja mediów dostarcza dodatkowego zabezpieczenia w przypadku awarii jednej z technologii. Bezpieczeństwo i integralność przesyłanych danych gwarantowana jest poprzez proces szyfrowania. Nasza sieć posiada również węzeł dostępu do publicznej sieci internet.

Banki Spółdzielcze SGB muszą nieustannie adaptować swoje strategie cyberbezpieczeństwa, aby zapewnić, że dostęp do internetu pozostanie bezpieczny, efektywny i zgodny z obowiązującymi regulacjami.

- Bezpieczny dostęp do internetu – W ramach usługi SGB-Bank umożliwia dostęp do zasobów w sieci internet. Zapewniony jest również odpowiedni poziom bezpieczeństwa poprzez:
  - kontrolę treści odwiedzanych stron,
  - pakiet bezpieczeństwa,
  - całodobowy monitoring dostępności usługi w trybie 24/7/365 i awarii,
  - łącze zapasowe oraz urządzenie zapasowe,
  - możliwość raportowania wykorzystania usługi przez pojedynczych użytkowników,
  - monitoring zdarzeń realizowany całodobowo przez SOC SGB,
- Bezpieczna Poczta SGB – To usługa poczty email oparta o narzędzia Microsoft Exchange. Usługa daje również dostęp do współdzielonych kalendarzy i zadań. Jej bezpieczeństwo zapewnia zestaw narzędzi chroniących przed spamem, malwarem i ransomwarem oraz ciągły nadzór realizowany przez SOC SGB.

Wspólne budowanie usług dostępu do internetu

przez banki spółdzielcze przy współpracy z bankiem zrzeszającym oferuje szereg korzyści strategicznych i operacyjnych.

Umożliwia to lepsze wykorzystanie zasobów poprzez dzielenie się kosztami rozwijania i utrzymania infrastruktury IT oraz systemów bezpieczeństwa.

Dzięki temu, nawet mniejsze banki spółdzielcze zyskują dostęp do zaawansowanych technologii i rozwiązań cyberbezpieczeństwa. Umożliwia to skorzystanie z doświadczenia banku zrzeszającego w zakresie bezpieczeństwa cyfrowego. Wspólne inicjatywy mogą prowadzić do standaryzacji procesów i procedur bezpieczeństwa, co ułatwia zarządzanie ryzykiem na poziomie całego zrzeszenia i zwiększa jego bezpieczeństwo.

Taka współpraca może stymulować innowacje, umożliwiając bankom spółdzielczym wprowadzanie nowoczesnych usług bankowości internetowej i mobilnej, które odpowiadają na rosnące oczekiwania klientów w zakresie dostępności i funkcjonalności cyfrowych usług finansowych. W ten sposób Banki Spółdzielcze SGB mogą lepiej konkurować na rynku, jednocześnie utrzymując wysoki poziom bezpieczeństwa.

Podsumowując, zapewnienie bezpiecznego dostępu do internetu i poczty e-mail w banku spółdzielczym jest fundamentalne dla ochrony przed cyberzagrożeniami. Wymaga to jednak ciągłej czujności, edukacji pracowników, strategicznych inwestycji w technologie bezpieczeństwa bądź skorzystania z oferty banku zrzeszającego. ●

Musimy przystosowywać **nowe technologie** do naszych lokalnych trendów

Rozmowa z **Jowitą Michalską**, prezeską Digital University, ekspertką w obszarze nowych technologii i kompetencji przyszłości

Czy nie ma pani wrażenia, że przy tak olbrzymim tempie rozwoju technologicznego mamy dziś do czynienia z dwiema grupami ludzi, nieproporcjonalnymi pod względem wielkości, które różni gigantyczna przepaść aktywności? Z jednej strony spora liczba technologicznych geeków, futurystów, specjalistów od sztucznej inteligencji, a z drugiej – wielomiliardowy zbiór ludzi, którzy wyłącznie przyglądają się temu postępowi i nie są aktywni w jego tworzeniu. Nie rozumieją go lub się boją. Czy podział na garstkę liderów i obojętną globalną większość służy rozwojowi?

Jowita Michalska: Zawsze było tak, że po jednej stronie istniały grupy świadomych liderów, nowatorów, którym zależy na zmianie. Ale są też ludzie, którzy po prostu chcą przeżyć i nie zgłaszają zainteresowania udziałem w rewolucjach. Teraz to rozwarstwienie się pogłębia, bo tematyka przeobrażeń technologicznych jest coraz bardziej skomplikowana. Zrozumieć mechanizmy kryptowalut, technologii blockchain czy dużych modeli językowych, z którymi się komunikujemy, to ogromna trudność.

Są specjaliści, którzy rozumieją nowe technologie, potrafią z nich korzystać i zarabiać na nich, ale przede wszystkim – tworzą je. Pozostali albo starają się nadążać albo są sparaliżowani strachem. Obawiają się świata cyfrowego, nie rozumieją go i są przekonani, że nigdy nie będą w stanie zrozumieć. To jest typowy lęk przed nieznanym, dlatego tak ważna jest rola edukacji. Na pewien podstawowy poziom technologii jesteśmy w stanie wejść wszyscy. Nowe technologie są intuicyjne, nigdy wcześniej tak intuicyjne nie były! Nie musimy być programistką/programistą, by projektować dla siebie odpowiednie narzędzia cyfrowe. Możemy mieć własnego chatbota, kupić go w sklepie OpenAI, który wkrótce będzie dostępny także w Polsce.

Za chwilę urządzenia zaczną rozmawiać między sobą, sztuczna inteligencja włączy robota gotującego, inną komendą uruchomi odkurzanie domu i suszenie prania – bo pani wraca z pracy! Futurologia? Nie. To nieodległa rzeczywistość.

Dajmy tu konkretny przykład. Potrzebuję asystentki, która będzie prowadziła moje media społecznościowe. Musi specjalizować się w tym obszarze, więc nie potrzebuję dużego modelu językowego, ale taki, który będzie bardzo dużo wiedział o tej jednej dziedzinie. Biorę ChatGPT, przygotowuję jego spersonalizowaną wersję, za którą płacę 20 dolarów miesięcznie – i customizuję ją, czyli piszę: będziesz moją asystentką, masz na imię Dorota, nie musisz mi mówić dzień dobry, ale umówmy się, że zwracasz się do mnie: *Hej, kapitanie!*

Daję jej zadanie – oto moje media społecznościowe, takim jestem człowiekiem, takie mam cele, o tym piszę, to mnie interesuje. Masz robotę: zaplanuj mi na kolejne dwa tygodnie tematykę postów i przygotuj terminarz publikacji. Napisz mi te wszystkie teksty, podaj w jakim medium chcemy je opublikować, stwórz do tego grafiki…

Mamy wszystko – w jednym cyfrowym narzędziu. Mogę tę moją Dorotę wysłać na szkolenie, poprosić o przeszukanie Sieci w celu znalezienia odpowiednich kwalifikacji i danych. Ona to zrobi, nauczy się. Mogę więc edukować swoją asystentkę, a ona będzie coraz lepiej wyspecjalizowana i stanie się dla mnie coraz większym wsparciem.

Mało tego, mogę zacząć na niej zarabiać! Mogę ją sprzedać, gdy już zdobędzie unikatową wiedzę, w postaci aplikacji poradniczej.

To wymaga jednak sporych umiejętności technologicznych...

Wcale nie tak wielkich! Przywykliśmy, że aplikacje tworzą twórcy, programiści, ludzie którzy kodują. Ale teraz, przy powszechnym do-

stępie do intuicyjnych narzędzi, nawet ja, osoba, która nigdy nie zajmowała się kodowaniem, może sama taką aplikację stworzyć.
I właśnie to zrobiłam, stworzyłam sobie taką asystentkę, specjalistkę od wzrostów na moich profilach w social mediach. Mogę ją wstawić do sklepu OpenAI i sprzedawać ludziom, którym nie chce się tworzyć własnej wersji asystenta, więc może pobiorą moją.
Wróćmy na moment do pytania, które zadał pan na początku naszej rozmowy. Owszem, jest garstka ludzi, bardzo mała, która tworzy te technologiczne nowe światy. Mamy dzięki niej olbrzymią i stale rosnącą alternatywną rzeczywistość z narzędziami, które pozwalają na dużo więcej niż dotychczas. Możemy wykreować dowolne wideo z nieistniejącymi fizycznie osobami. One będą śpiewały, biegały, przemawiały do nas. Wszystko, co chcemy. Zaczynamy tworzyć rzeczywistość alternatywną wobec naszej, której doświadczamy na co dzień.
A z drugiej strony – właśnie dzięki takim narzędziom dosłownie każdy może stać się twórcą. ChatGPT i inne tego rodzaju modele językowe stają się coraz lepsze, ponieważ uczą się dzięki naszemu próbowaniu. Można nie przejść żadnego szkolenia, ale dzięki intuicyjności rozwiązań świetnie wykorzystywać technologię. Rzecz jasna warto czytać, uczestniczyć w specjalistycznych webinariach, wchodzić na podcasty i poszerzać swoją wiedzę, bo nigdy jej za dużo. W ten sposób dużo szybciej pokonamy lęk i dużo efektywniej wykorzystamy dostępne instrumenty.

Które trendy w rozwoju technologicznym będą miały wpływ na rozwój polskich firm w najbliższych latach? Sztuczna Inteligencja? Robotyka i automatyzacja procesów? A może zupełnie inny element – wiedza i edukacja pracowników, ich motywacja, zdrowie, wellbeing?

Mamy wielką zmianę w myśleniu o trendach. Pierwsze dwa-trzy lata mojej praktyki w tym zakresie były proste. Istniały tzw. megatrendy, duże, było ich pięć, dziesięć, dwanaście, harmonijnie się ze sobą łączyły.
Dzisiaj – w świetle ogromnych i błyskawicznych zmian technologicznych – muszę wybierać dla jednej organizacji spośród dwustu-trzystu mikro- i makrotrendów! Wszystkie one mogą mieć wpływ, same lub w powiązaniu z innymi, na działalność organizacji lub przedsiębiorcy.

Rzecz jasna warto czytać, uczestniczyć
w specjalistycznych webinariach, wchodzić
na podcasty i poszerzać swoją wiedzę,
bo nigdy jej za dużo.

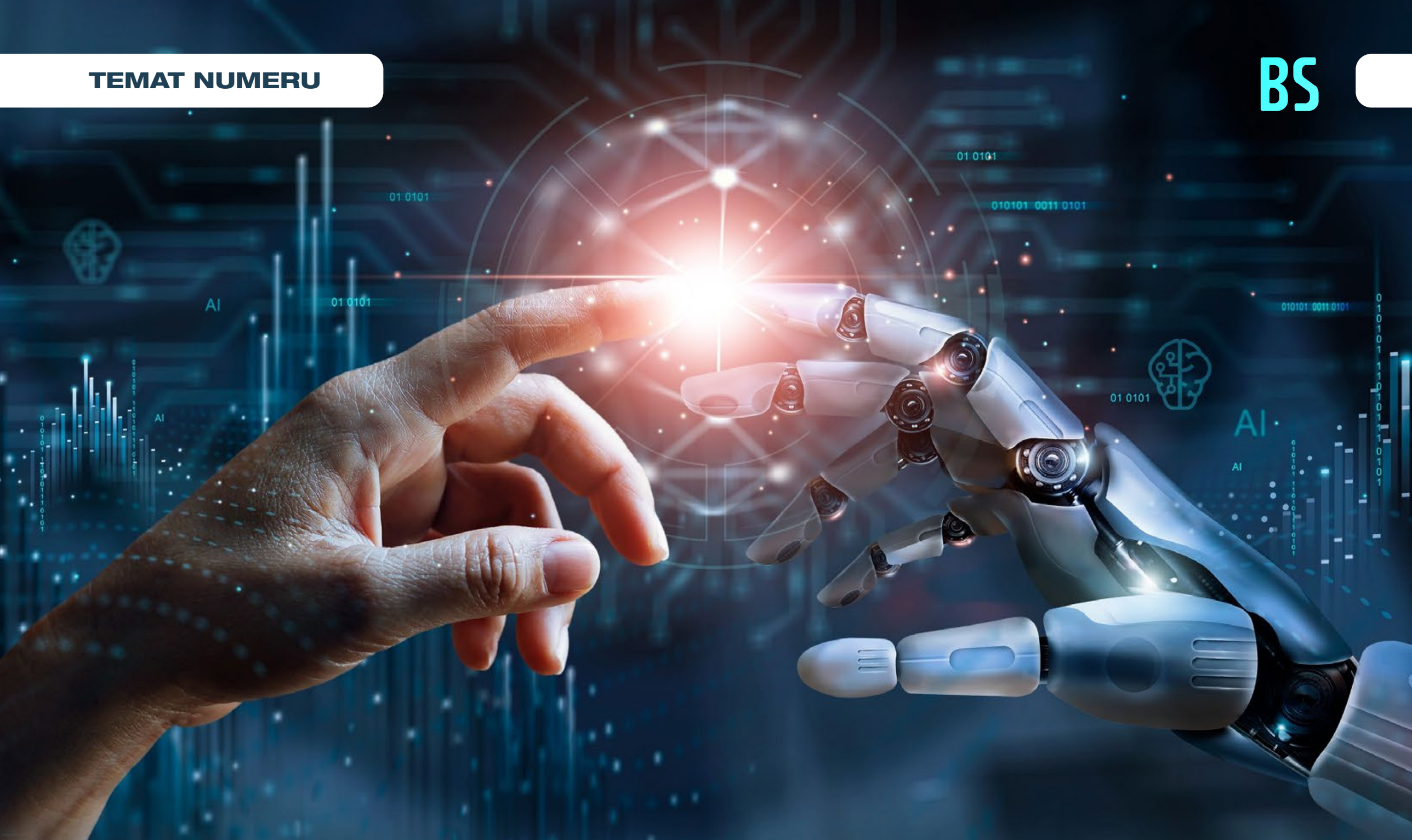
Jednym z trendów jest przechodzenie z poziomu device na multidevice. Kiedyś mieliśmy komputer, aparat, odtwarzacz mp3, kalkulator, latarkę, konsolę do gier, a potem wszystko to wchłonął smartfon – i znaleźliśmy się w zupełnie innym świecie. Dawniej musieliśmy się nauczyć fotografii, by robić zdjęcia, a teraz po prostu naciskamy punkcik na ekranie smartfona i algorytmy wykonują za nas całą pracę. Ze smartfona uruchamiamy ogrzewanie, pralkę, światła w pokoju, muzykę czy domowe kino.

Warto więc nie gniewać
się na technologie
i być małym bankiem
z dużą technologią,
a jednocześnie
pielęgnować personalne
relacje.

Ale zaczyna się także trend odwrotny – specjalizacja sprzętów. Mamy smartwatche albo inne urządzenia z gatunku IoT, które mierzą puls i poziom tlenu we krwi, liczą kroki, oddechy, mierzą głębokość snu, poziom hałasu i potrafią wykonać szybkie EKG, a wszystko to robią bardzo profesjonalnie, czasami na poziomie laboratoryjnym. Są okulary, lekkie i wygodne, które korygują nam wzrok, a jednocześnie stanowią ekran, na którym wyświetlamy informacje, maile, komunikaty z mediów społecznościowych, ale też elementy rozszerzonej rzeczywistości.
W najbliższych pięciu latach robotyzacja i automatyzacja na pewno będą rozwijały się bardzo dynamicznie. Widzimy, co robi Tesla, są wielkie projekty konwergencji sztucznej inteligencji z coraz sprawniejszymi fizycznie robotami, które już nie tylko wchodzą do fabryk – co jest faktem od lat – ale też częściej goszczą w naszych domach. Mamy robota Samsunga, który opiekuje się psem i kiedy widzi, że zwierzę się nudzi lub tęskni, włącza mu muzykę, kreskówki w telewizorze albo otwiera drzwi do ogrodu.
Z jednej strony mamy zatem Industry 4.0 czy już wręcz Industry 5.0 podnoszące na wyższy poziom komunikację ludzi z maszynami, a z drugiej coraz mądrzejsze są na przykład roboty sprzątające czy zmywające. Sama czekam na robota, który przejmie za mnie stery w kuchni. Całkiem serio wyobrażam sobie tę chwilę, kiedy wejdę do domu, zagadam do jakiegoś multimodalnego modelu sztucznej inteligencji – hej, trzeba coś ugotować, zobacz co mamy w lodówce i ugotuj jakiś szybki obiad. I niech wymyśli, co wybrać dla moich sześciorga domowników, z których każdy ma alergię na coś innego…
Za chwilę te urządzenia zaczną rozmawiać między sobą, sztuczna inteligencja włączy robota gotującego, inną komendą uruchomi odkurzanie domu i suszenie prania – bo pani wraca z pracy! Futurologia? Nie. To nieodległa rzeczywistość.

Jowita Michalska
Prezeska Fundacji
Digital University

Manager z prawie 20 letnim doświadczeniem na rynku marketingu i mediów. Swoją karierę rozpoczynała w latach dziewięćdziesiątych na prężnie rozwijającym się rynku międzynarodowych agencji reklamowych.
Odpowiadała za wielokrotnie nagradzane kampanie reklamowe: m.in. Heyah, a potem Plus z kabaretem Mumio. Obecnie działa w Fundacji FSCD Polska zajmującej się m.in. edukacją w zakresie nowych technologii oraz rozwoju osobistego.
Zasiada w radach i jury różnych instytucji i projektów. Jej pasją są media społecznościowe i ich wpływ na zmiany w globalnej komunikacji, a także wpływ nowych technologii na modele biznesowe.



Nie musimy być programistką/programistą, by projektować dla siebie odpowiednie narzędzia cyfrowe. Możemy mieć własnego chatbota, kupić go w sklepie OpenAI, który wkrótce będzie dostępny także w Polsce.

Patrząc przez pryzmat rzeczywistości małych i średnich firm, a nie globalnych korporacji – czy potrafimy wykorzystywać nowe technologii dla potrzeb właśnie mikrobiznesu?

Gdzie jest wyzwanie? W rozumieniu zasad rozwoju i wykorzystania narzędzi. Mamy dwóch przedsiębiorców, pana A i pana B. Ten pierwszy korzysta z pełnego instrumentarium nowych technologii, a pan B – nie. Możemy mieć pewność, że pan A jest o 20-40 procent efektywniejszy od pana B. W biznesie to bardzo dużo. Pan A lepiej zarabia, ma mniej roboty, szybciej się rozwija. I jeśli kiedyś pan A spotka się na długiej rozmowie z panem B, to jestem pewna, że nastawienie tego drugiego zmieni się szybko i mocno, bo nikt nie lubi zostawać z tyłu. Każdy chce wygrywać.

Problem tkwi w czymś innym – wiele osób szybko się poddaje. Wyzwaniem jest to, że ktoś spróbował raz i mówi – to jest głupie, nie ogarniam. Obrona przed nowym: jak się czegoś boimy, to mówimy, że jest głupie.

Ale i tutaj coś się zmienia. Widzę ogromny wzrost zainteresowania tematem AI. Moje media społecznościowe prowadzę hobbystycznie, żeby dzielić się wiedzą, i one były dotychczas niezwykle niszowe. Obserwowali mnie ludzie głównie z mojego środowiska. Teraz widzę skok zainteresowania, codziennie przybywa kilkuset nowych followersów. To znaczy, że ich zapotrzebowanie na ten rodzaj wiedzy dynamicznie rośnie. Jeszcze dwa lata temu myśleli, że AI jest nie dla nich – dziś zmienili optykę.

Co pani zdaniem mogą zrobić małe lokalne banki, których możliwości technologiczne i finansowe są ograniczone, by skutecznie rywalizować na rynku z gigantami?

Czy siła jest w lokalności? Czy mały bank ma szansę lepiej poznać potrzeby swojego klienta właśnie z uwagi na bezpośredniość relacji? Dwa wątki tu widzę. Pierwszy – musimy przystosowywać nowe technologie precyzyjnie do naszych lokalnych trendów, potrzeb i uwarunkowań. Małe organizacje potrafią dużo, bo działają zwinnie, sprawnie, szybko mogą dostosować się do nowych warunków. Mogą błyskawicznie dostrzec tzw. pain pointy, czyli miejsca najbardziej bolesne i szybko zaadresować swoją ofertę lub pomoc. Jeśli ich pracownicy są odpowiednio zainspirowani, przeszkoleni, dobrze zmotywowani, mogą sobie z takimi problemami poradzić.

Czy jednak bankowcy, którzy mają osobiste relacje z klientami wiedzą o nich więcej niż pracownicy dużych banków, dysponujący potężnymi zasobami technologicznymi? Tu bym się spierała. Pamiętajmy, że wiele naszych zachowań nie jest uświadomionych, nie werbalizujemy ich przed nikim, nawet rodziną, a co dopiero przed pracownikiem banku. Jeśli bank w czasie rzeczywistym potrafi dobrze przeanalizować dane na temat swojego klienta – bo pozwala mu na to technologia cyfrowa – to wie o nim dużo więcej niż bank nastawiony wyłącznie na relacje bezpośrednie. Duża konkurencja ma przewagę w swojej sile technologicznej, zdolnościach analitycznych. I łapie klienta dokładnie wtedy, kiedy on zaczyna odczuwać jakąś konkretną potrzebę. Albo wręcz ją wyprzedza.

Ręcznie sterowany klient, który wpada do oddziału banku, z którym czasem sobie pogadamy, czasem damy mu jakiś gift lub złożymy życzenia świąteczne, niekoniecznie nam powie, że właśnie szuka w sieci nowej kosiarki, ale nie ma na nią wystarczająco dużo pieniędzy…

Oczywiście, te relacje bezpośrednie zawsze będą miały swoją wartość – ja ich nie deprecjonuję i uważam, że w zautomatyzowanym świecie ludzie będą jednak chcieli wracać do ciepłych, bliskich kontaktów i do tego, że pani z banku pamięta o urodzinach i wysyła sympatyczne życzenia.

To ma wartość. Ale musi iść w parze z technologią, bo poziom wiedzy, którą z naszych danych może wyczytać duży integrator i jego systemowe narzędzia analityczne, jest niewspółmierny do tego, co możemy osiągnąć wyłącznie na podstawie rozmowy bezpośredniej. Warto więc nie gniewać się na technologie i być małym bankiem z dużą technologią, a jednocześnie pielęgnować personalne relacje. Te dwie ścieżki działania dadzą najlepszy efekt… One się świetnie uzupełniają. ●

Rozmawiał: Jacek Prześluga

PODCAST SPÓŁDZIELCZY SGB

KLIKNIJ ŻEBY POSŁUCHAĆ ARTYKUŁU

Walka z fake newsami i dezinformacją

Jak dobry content pomaga w odróżnieniu prawdy od fikcji?

Agnieszka Szelejewska
Content manager w takaoto.pro

Fake newsy – te małe, złośliwe kłamstewka, które rozprzestrzeniają się szybciej niż plotki o podwyżce w pracy, mają niezwykłą moc: wpływają na nasze decyzje, emocje, postrzeganie świata. Czy dobra, solidna dawka faktów może być równie wciągająca, jak ostatni sezon ulubionego serialu? Owszem! Nasza przygoda zaczyna się właśnie tutaj, w krainie dobrego contentu. Zapraszam w podróż po meandrach prawdy i fikcji, w której każdy może stać się detektywem własnych przekonań.

Social media: główne źródło epidemii dezinformacji

Zastanów się przez chwilę: ile razy zdarzyło ci się podzielić „newsem", który później okazał się kompletną bzdurą? Według badań przeprowadzonych w 2023 r. przez YouGov, aż 23% Amerykanów co najmniej raz udostępniło fałszywą informację[1]. Z tego samego raportu wynika, że ponad połowa danych w internecie jest fałszywa, a 86% obywateli dosięgają fake newsy, z czego 3 na 10 osób w nie wierzy. Głównym źródłem nieprawdziwych informacji są media społecznościowe, co potwierdza 67% respondentów. To w głównej mierze z nimi walczymy o przestrzeń dla prawdy i rzetelności.

Czym jest fake news i dezinformacja

Zacznijmy od podstaw: czym są fake newsy? To fałszywe informacje produkowane i rozprzestrzeniane z różnych powodów – od niewinnych żartów po świadome próby wpłynięcia na opinię publiczną czy rynek finansowy. Ich znakiem rozpoznawczym jest forma, która naśladuje wiarygodne źródła informacji, np. artykuły prasowe, wiadomości telewizyjne itp. Apogeum fake newsów przeżywaliśmy m.in. podczas pandemii COVID-19.

Z kolei dezinformacja to nieco szersze pojęcie. Obejmuje ono także zmanipulowane zdjęcia, wideo, sfabrykowane statystyki, twierdzenia oraz inne dane. Stanowi potężne narzędzie w wojnie informacyjnej, co dobitnie widzimy na przykładzie działań Rosji związanych z jej inwazją na Ukrainę.

Jakie zagrożenia mogą wyniknąć z dezinformacji?

Niektóre kategorie fake newsów mogą być szczególnie niebezpieczne. Należą do nich m.in. te związane z medycyną: zastosowanie się do ich wskazań grozi utratą zdrowia, a nawet życia. Szczególnie szkodliwa jest także taka dystrybucja fake newsa, która ma na celu wyłudzenie od ofiar środków finansowych. Inne mogą przybierać znacznie łagodniejszy obrót, zawsze wprowadzając jednak absolutny zamęt w danych środowiskach. Przykład z branży finansowej?

Wyobraź sobie, że w internecie zaczyna krążyć plotka o bankructwie pewnej poważnej firmy. Zanim ktokolwiek zdąży zweryfikować te doniesienia, wartość jej akcji niebezpiecznie pikuje, w akcie paniki zmuszając inwestorów do wyprzedaży swoich udziałów. Po krótkim czasie okazuje się jednak, że ta informacja była równie prawdziwa, co… plotka o tym, że Elvis żyje i właśnie został mianowany prezesem banku centralnego.

A co jeśli ktoś opublikuje sfabrykowany raport o kondycji rynków finansowych? W mgnieniu oka ekonomiści, inwestorzy, a nawet przypadkowi przechodnie zamieniają się w ekspertów od rzekomej bańki spekulacyjnej, która w rzeczywistości okazuje się nie więcej niż bańką mydlaną.

Każda dezinformacja może mieć poważne konsekwencje. Tworzy alternatywny wszechświat, w którym plotki są bardziej wartościowe niż fakty. Zamiast ulegać panice wywołanej przez fake newsy, warto uzbroić się w zdrowy sceptycyzm i dozę starego dobrego fact-checkingu. Na czym on polega?

Metody walki z dezinformacją

Naszym najlepszym sprzymierzeńcem w walce z dezinformacją jest fact-checking, czyli metoda dociekania prawdy poprzez przeszukiwanie wiarygodnych źródeł, dokumentów, danych statystycznych, badań naukowych itp. Gdy fact-checkerzy odnajdą potrzebne informacje, porównują je z tym, co zostało przedstawione w wątpliwym twierdzeniu. Jeśli fakty się zgadzają, światło zielone – informacja jest prawdziwa. Jeśli

Walka z dezinformacją i fake newsami odbywa się także poprzez edukację społeczną.

jednak odkryją nieścisłości, zapala się czerwona lampka ostrzegawcza: informują o tym publikę, by nikt inny nie dał się zwieść. Na świecie działa wiele organizacji i inicjatyw zajmujących się fact-checkingiem. Do jednych z popularniejszych należą m.in. Snopes, FactCheck.org czy PolitiFact, a w Polsce np. Demagog.

Walka z dezinformacją i fakenewsami odbywa się także poprzez edukację społeczną. Liczne programy, kursy czy webinary uczą,

[1] https://www.demandsage.com/fake-news-statistics/

jak rozpoznawać nieprawdziwe informacje, zwracać uwagę na źródło i kontekst, a także jak korzystać z narzędzi do weryfikacji faktów.

Nie mniejszą rolę w dementowaniu nieprawdziwych plotek odgrywają nowoczesne technologie, w tym sztuczna inteligencja. Algorytmy automatycznie wykrywają i flagują podejrzane treści. Ponadto AI potrafi analizować ogromne ilości danych w krótkim czasie, co znacznie przyspiesza proces fact-checkingu. Instagram aktywnie zwalcza dezinformację poprzez ograniczanie zasięgu wprowadzających w błąd treści oraz blurowanie, czyli rozmazywanie obrazów, które zostały celowo poddane obróbce graficznej, by zafałszować rzeczywistość (deepfake). Google także wypowiedział wojnę dezinformacji. Regularnie aktualizuje swoje algorytmy, by witryny oferujące rzetelne informacje były wyżej w wynikach wyszukiwania.

Istnieją także regulacje prawne mające na celu zwalczanie dezinformacji. Za rozpowszechnianie fake newsów grożą dwa rodzaje odpowiedzialności: cywilna oraz karna. Z tytułu tej pierwszej ofiara fake newsa może zażądać zaprzestania naruszania jej dóbr osobistych wynikających z art. 23 Kodeksu cywilnego[2], usunięcia jego skutków i zadośćuczynienia pieniężnego. Sprawca może ponieść odpowiedzialność karną za zniesławienie lub zniewagę, nawet trafiając do więzienia. Legislacja kwestii fake newsów jest jednak przedmiotem nieustannej dyskusji i budzi poważne kontrowersje. Całkowity zakaz dystrybucji nieprawdziwych informacji w praktyce oznaczałby bowiem naruszenie podstawowego prawa do wolności słowa i równałby się z wprowadzeniem cenzury.

Nie zadzieraj z Google!

Wróćmy na moment do giganta z Mountain View. Wspominałam, że stał się ważnym sojusznikiem w walce z dezinformacją dzięki wprowadzeniu strategii mających na celu promowanie rzetelnych treści oraz ograniczanie rozprzestrzeniania się fałszywych informacji. W tym kontekście warto wspomnieć o kluczowej koncepcji: E-E-A-T (Expertise, Experience, Authoritativeness, Trustworthiness – Ekspertyza, Doświadczenie, Autorytet, Wiarygodność). O co tutaj chodzi?

Treści powinny być tworzone przez ekspertów z danej dziedziny, odzwierciedlać ich doświadczenie i głębokie zrozumienie tematu. Ekspertyza i autorytet zapewniają, że informacje są rzetelne, podczas gdy doświadczenie dodaje unikalności, świeżej perspektywy i praktycznej wiedzy. Wiarygodność zaś gwarantuje, że treści są godne zaufania, a stwierdzenia tam zawarte są zgodne z prawdą, a więc i bezpieczne dla użytkowników.

W skrócie: aby content był zgodny z zasadą E-E-A-T, powinien być oryginalny, pomocny, napisany przez ludzi i dla ludzi, zawierać informacje o autorze oraz korzystać z wiarygodnych źródeł – zwłaszcza jeśli dotyczy sektorów YMYL.

Czym z kolei jest YMYL? To akronim od Your Money or Your Life – „pieniądze albo życie”. Odnosi się do treści mających bezpośredni wpływ na finansową stabilność, zdrowie, bezpieczeństwo czy dobrostan odbiorców treści. Google traktuje te treści z większą ostrożnością, wymagając wyższych standardów E-E-A-T, aby upewnić się, że użytkownicy mają dostęp do informacji najwyższej jakości i najbardziej wiarygodnych źródeł. Dąży zatem do stworzenia zdrowszego ekosystemu informacyjnego, w którym jakościowy content jest łatwo dostępny, a dezinformacja marginalizowana.

Głównym źródłem nieprawdziwych informacji są media społecznościowe, co potwierdza 67% respondentów. To w głównej mierze z nimi walczymy o przestrzeń dla prawdy i rzetelności.

Dobry content w branży finansowej jako kompas w dżungli dezinformacji

Biorąc na tapet branżę finansową, sprawdźmy, jak dobry content może pomóc w odróżnieniu prawdy od fikcji:

- Wiarygodność i transparentność źródeł – banki powinny publikować raporty i analizy z dokładnymi odnośnikami do źródeł danych, zachęcając klientów do samodzielnej weryfikacji faktów.
- Edukacja i rozwijanie krytycznego myślenia – poprzez dystrybucję edukacyjnych treści: webinariów, kursów e-learningowych na temat zarządzania finansami osobistymi, inwestycji czy ryzyka kredytowego, instytucje finansowe ułatwią zrozumienie skomplikowanych mechanizmów rynkowych.
- Unikanie jednostronnej narracji – przedstawianie zróżnicowanych perspektyw w treściach finansowych zapewni głębsze zrozumienie rynku. Mogą to być różne scenariusze ekonomiczne z bogactwem możliwości i ryzyk, co z pewnością wesprze klientów w świadomym podejmowaniu decyzji inwestycyjnych.
- Używanie prostego i zrozumiałego języka – wysokiej jakości treści nie mają nic wspólnego z zawiłym, bełkotliwym językiem – w bankowości nazywanym „bankishem”. Dobry content powinien tłumaczyć trudne koncepcje w sposób jasny (np. poprzez infografiki czy objaśnienia wideo), co sprawi, że odróżnienie faktów od fikcji będzie możliwe dla ogółu, a nie tylko dla ekspertów.
- Interaktywność i angażowanie odbiorców – skutecznym narzędziem edukacyjnym w branży bankowości mogą być treści, które zachęcają do interakcji. Przykład? Quizy weryfikujące wiedzę czy kalkulatory służące modelowaniu różnych scenariuszy finansowych. Informacje podane w ten sposób staną się bardziej zrozumiałe, a na dodatek zachęcą do myślenia krytycznego i nieakceptowania informacji bez osobistej analizy.

Jaki jest zatem dobry content?

Z jego pomocą łatwiej odróżnić fakty od fikcji. Dobry content nie tylko informuje, ale i edukuje – i to w sposób daleki od nudnych wykładów czy encyklopedycznych rozważań, które szybko usypiają czujność czytelnika. Służy jako solidny fundament dla naszego krytycznego myślenia. Jest jak przewodnik po skomplikowanym świecie informacji, pomagając nie tylko zrozumieć, co jest prawdą, ale także dlaczego coś jest fałszem. Dzięki niemu stajemy się nie tylko konsumentami informacji, ale jej świadomymi kuratorami gotowymi rozprawić się z dezinformacją jednym, dobrze wymierzonym kliknięciem. ●

[2] https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-cywilny-16785996/art-23

Ciemna strona cyfryzacji

Prof. dr hab. Jarosław Liberek
językoznawca, kierownik Telefonicznej Poradni Językowej na UAM

Jakkolwiek to dziwnie zabrzmi, to jednak w przypływie wisielczego humoru można powiedzieć, że złodzieje zawsze szli z duchem czasu. Kiedyś po prostu zabierali i szybko uciekali, co wymagało sprytu i zdolności fizycznych. Jeszcze niedawno udawali inkasentów, dobrotliwych przyjaciół dawno niewidzianego wnuczka, zatroskanych policjantów oferujących pomoc. W dalszym ciągu udają i podszywają się, ale chyba rzadziej, bo dzisiejszy „cyfrowo oprzyrządowany" przestępca woli działać „innowacyjnie". Bez wychodzenia z bloku w jakimś Marianowie Górnym (a przede wszystkim bez wstawania od komputera!) może okraść zarówno sąsiada zza ściany, jak i Bogu ducha winnego pana Pedro Pablo Ramireza z Argentyny.

Z oczywistych powodów cyberkradzieje

często zakładają fikcyjne strony banków oraz preparują niby autentyczne e-maile i esemesy z tych instytucji. Zasada ogólna jest dość prosta: wszystko ma do złudzenia przypominać prawdziwą stronę i autentyczne komunikaty. Stworzenie fałszywych obrazów i treści nie jest trudne. Strony banków i wysyłane przez nie informacje są powszechnie dostępne. Nie trzeba być wybitnym grafikiem komputerowym czy lingwistą, aby podróbki sprawiały wrażenie od początku do końca prawdziwych. Złodzieje wykorzystują podstawowe zasady komunikowania przy użyciu złożonych struktur znakowych. Oszukiwana ofiara odbiera te struktury automatycznie i zazwyczaj nie zauważa, że od tych oryginalnych jednak się różnią, choć te różnice są minimalne.

Nikczemny proceder udaje się, ogólnie rzecz biorąc, z dwóch powodów. Po pierwsze, odwieczną i powszechną cechą każdego aktu komunikacyjnego jest swoista wybiórczość, połączona z koncentracją na istocie rzeczy. Chodzi o to, że człowiek, do którego dochodzi komunikat, nie odbiera wszystkich jego szczegółów, ale tylko te, które są istotne informacyjnie. Gdyby dany osobnik analizował każdą drobnostkę obrazów i tekstów, percypowałby je długo, a jego magazyn przechowujący dane, czyli mózg, szybko by się zapełnił i zaczął odbijać wiadomości, jak przepełniona skrzynka poczty elektronicznej. Selektywność percepcyjna to swoisty paradoks, bo przecież żeby zrozumieć, powinniśmy w zasadzie wszystko przyjąć, tymczasem w praktyce tak nie jest i żeby zrozumieć, pomijamy pewne szczegóły. Właśnie tak rozumianą wybiórczość wykorzystują cyberprzestępcy. Wiedzą, że człowiek nie będzie przez lupę czytał fałszywej strony i nie zauważy kilku detali, które będą ją odróżnić od tej niefałszywej. Diabeł tkwi w szczegółach, w przypadku podstawionych stron w jakimś pojedynczym ukośniku zamiast podwójnym, w dodatkowej kropce lub niby zgubionej kresce.

Druga przyczyna ułatwiająca złodziejom zadanie wynika z okoliczności, którą można umownie określić mianem przytłoczenia cyfrowością. Żyjemy w świecie wypełnionym po brzegi technologią. Wielu ludzi nie odnajduje się w tym wszystkim. Czują się zagubieni w przestrzeni pulsujących ekranów, tablic, smartfonów i wyświetlaczy. Tzw. „wykluczenie cyfrowe", zbanalizowane przez propagandę medialną, w dużym stopniu do nich pasuje. Trudno się dziwić, że tacy zdezorientowani ludzie, świadomi swoich ograniczeń, żyjący pod presją wszechogarniających technologii, próbują nieraz nadążać, a próbując za wszelką cenę, nieco bezmyślnie i na swoje nieszczęście klikają.

Przyjęło się sądzić, że przytłoczenie cyfrowością jest głównie udziałem pokoleń średnich i starszych. Czyżby młodym, nierozumiejącym, dlaczego ludzie mówili kiedyś do siebie „przekręć do mnie", cyberprzestępcy nie zagrażali? Oczywiście zagrażają, bo w coraz bardziej technologiczną rzeczywistość wchodzimy globalnie, gromadnie i samochcąc. Problem w tym, że ci, którzy sprzedają jasną stronę cyfrowości, jednocześnie streczą jej ciemną

> Żyjemy w świecie wypełnionym po brzegi technologią.

stronę, przyczyniają się do naszego zagubienia i zwiększają ryzyko ponoszenia przez nas szkód. Stąd też, ci sami, oferują w pakiecie różne programy anty- i zabezpieczenia, potęgując złudne poczucie bezpieczeństwa, w konsekwencji więc osłabiają ludzką czujność i jak w błędnym kole ponownie zwiększają ryzyko strat itd.

Nie mnie orzekać, czy pani z okienka w banku zniknie całkowicie. Wiem jednak, że od szybko postępującej cyfryzacji nie ma odwrotu. Jestem też pewny, że narzekanie na jakichś „onych", które znowu coś w tym komputerze „wymyśliły", to ślepa uliczka. Potęga niesztucznej inteligencji jest wciąż ogromna. Wypada tylko przypomnieć, by wszyscy korzystali w pełni z tej potęgi i ze zgubionej w technologicznym pędzie starej, poczciwej cnoty roztropności. ●

Higiena cyfrowa

– zadbaj o bezpieczeństwo Twojej strony www

Krzysztof Swoboda
Technical Content Manager w Takaoto.pro

Higiena cyfrowa to jeden z fundamentów bezpieczeństwa. Warto podkreślić, że nie dotyczy ona tylko Twoich mediów społecznościowych czy aplikacji. W świecie biznesu niezwykle ważne jest odpowiednie zabezpieczenie Twojej strony www – bez względu na to, czy jest to blog czy serwis przedsiębiorstwa, którym zarządzasz. Na jakich obszarach musisz się skupić? Czy naprawdę tak trudno zadbać o bezpieczeństwo Twojej witryny w cyberprzestrzeni?

Podstawowe pojęcia i znaczenie bezpieczeństwa cyfrowego

Zrozumienie higieny cyfrowej zaczyna się od jej definicji. Jest to zbiór praktyk i procedur, których wdrożenie ma uchronić Twój serwis przed wieloma różnymi zagrożeniami: od kradzieży haseł, przez phishing, aż po przejęcie kontroli nad stroną i dodaniem jej do listy spambotów.

O bezpieczeństwo możesz zadbać na trzech różnych płaszczyznach:

- technicznej,
- praktycznej,
- organizacyjnej.

Ta pierwsza to np. aktualizowanie oprogramowania (CMS-a), które nią zarządza. Bezpieczeństwo praktyczne to włączenie weryfikacji dwuetapowej czy zastosowanie długich, trudnych do odgadnięcia haseł. Wymiar organizacyjny może polegać np. na szybkim reagowaniu na zagrożenia, o których informują portale branżowe. Okazało się, że wtyczka, z której korzystasz, ma lukę bezpieczeństwa? Zaktualizuj ją lub dezaktywuj. Lepiej nie kusić losu.

Ile warte jest cyberbezpieczeństwo? Co najmniej 6 miliardów dolarów!

Statystyki dotyczące naruszeń bezpieczeństwa są jednoznaczne: roczne globalne straty powstałe w wyniku włamań na strony WWW i kradzieży danych oszacowano na co najmniej 6 miliardów dolarów.

Zwróć też uwagę na to, że szczególnie zagrożone są darmowe, ogólnodostępne – a więc niezwykle popularne – CMS-y (jak chociażby WordPress). Według danych Patchstack liczba zgłoszonych luk bezpieczeństwa we wtyczkach WordPress wzrosła o 328% w porównaniu do 2021 roku, z 1,382 do 4,528 potwierdzonych błędów bezpieczeństwa. Większość z tych luk (93%) dotyczy właśnie pluginów. Nieco ponad 6% włamań udało się przeprowadzić poprzez źle zabezpieczone motywy graficzne.

WP Mayor szacuje, że rokrocznie przestępcy przejmują kontrolę nad 4 milionami stron pracującymi pod kontrolą WordPressa. Oznacza to, że każdego dnia hakowanych jest niemal 12 tysięcy serwisów. Inne platformy, jeśli nie są odpowiednio zabezpieczone i aktualizowane, również mogą paść ofiarami cyberprzestępców. Pamiętaj, że hakerzy mają do dyspozycji wiele różnych metod, by wykraść Twoje dane lub przejąć kontrolę nad witryną, którą zarządzasz. Do najpopularniejszych należą:

- malware,
- ataki phishingowe,
- ataki DDoS,
- oszustwa polegające na wykorzystaniu inżynierii społecznej i sztucznej inteligencji.

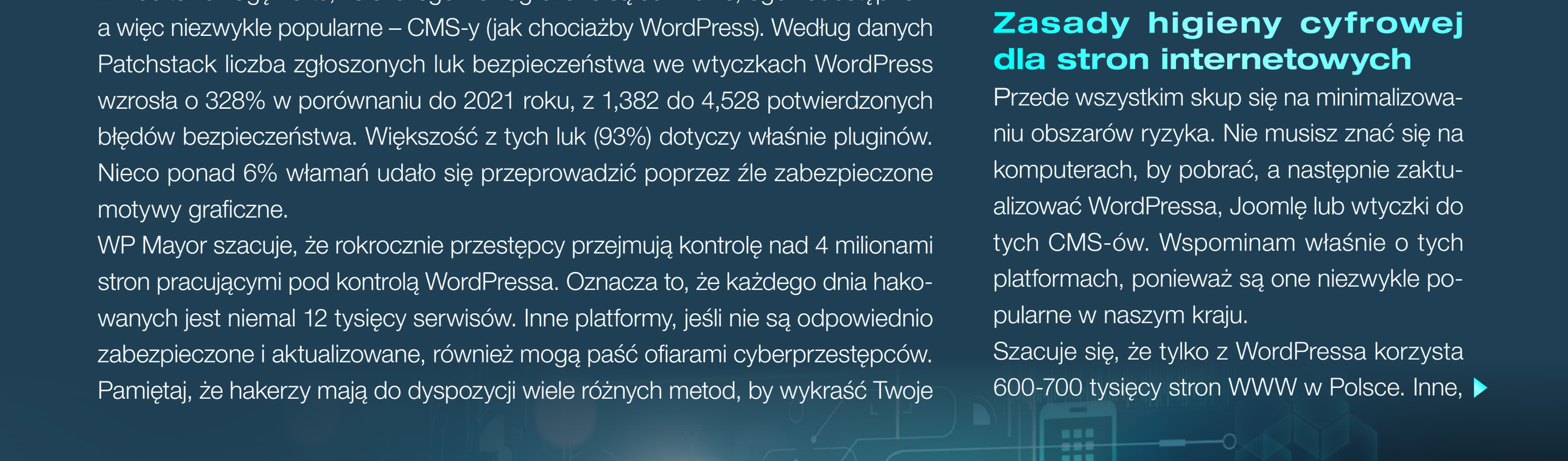
Jednym z najbardziej spektakularnych przypadków naruszenia bezpieczeństwa był atak na Equifax w 2017 roku, który ujawnił dane osobowe niemal 147 milionów osób. Ten przypadek pokazuje, jak zaniedbania w aktualizacji oprogramowania mogą prowadzić do katastrofalnych w skutkach wycieków danych.

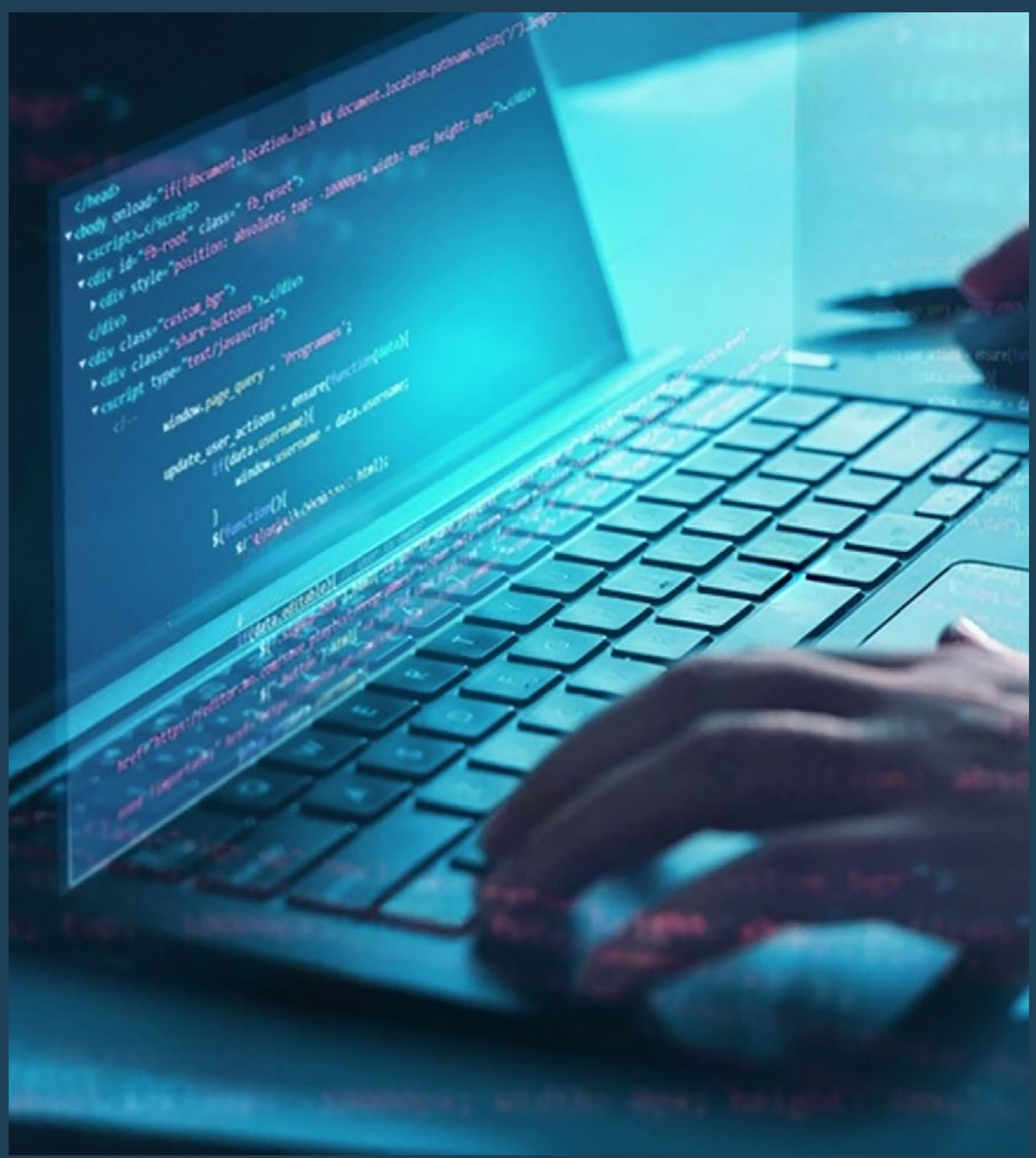
Cyberprzestępcy wykradli nie tylko numery 209 tysięcy kart kredytowych, ale i niemal kompletne dane osobowe setek tysięcy Amerykanów. Straty były ogromne, a przedsiębiorstwo musiało wypłacić ponad 700 milionów dolarów odszkodowań. Jest więc się czego obawiać.

Zasady higieny cyfrowej dla stron internetowych

Przede wszystkim skup się na minimalizowaniu obszarów ryzyka. Nie musisz znać się na komputerach, by pobrać, a następnie zaktualizować WordPressa, Joomlę lub wtyczki do tych CMS-ów. Wspominam właśnie o tych platformach, ponieważ są one niezwykle popularne w naszym kraju.

Szacuje się, że tylko z WordPressa korzysta 600-700 tysięcy stron WWW w Polsce. Inne, ▶





niszowe platformy, jak Drupal czy Bitrix również nie będą wymagać od Ciebie skomplikowanych, czasochłonnych czynności.

Aktualizacja CMS-a, czyli systemu, który zarządza Twoją stroną w sieci, jest tak prosta jak zainstalowanie nowego uaktualnienia do Windowsa lub iPhone'a.

Kluczowe obszary, dzięki którym możesz skutecznie chronić swoją stronę, to:

- regularne aktualizacje CMS-a oraz wtyczek i narzędzi webowych, które mają dostęp do danych administratora,
- stosowanie silnych haseł, unikalnych dla każdego konta. Zacznij używać aplikacji przypominającej o tym, by zmienić hasło. Przykłady takiego oprogramowania to: 1Password, Keeper i NordPress,

Bez względu na to, czy prowadzisz bloga czy duży sklep online lub portal, który pozwala na tworzenie kont użytkowników i gromadzi o nich wiele danych, musisz zadbać o higienę cyfrową takiego projektu.

- wdrożenie na stronie dodatkowego uwierzytelniania MFA – po podaniu hasła na podany podczas rejestracji numer telefonu lub adres e-mail zostanie wysłany kod, który należy wprowadzić w ciągu 60 sekund. To dodatkowy bufor bezpieczeństwa, z którego powinny skorzystać te osoby, które często logują się do swojej strony z publicznych sieci Wi-Fi,
- certyfikat SSL. Dziś to właściwie standard, dzięki któremu Twoje dane są chronione silnym, zazwyczaj 256-bitowym kluczem symetrycznym, który znacznie utrudnia przejęcie kontroli nad stroną. Możesz skorzystać z darmowego certyfikatu Let's Encrypt lub wykupić wersje płatne, na przykład RapidSSL.

Niezwykle ważną kwestią, która wpływa na bezpieczeństwo Twojej strony WWW, są też cykliczne audyty bezpieczeństwa. Niektóre firmy świadczą taką usługę online. Jeśli jednak zarządzasz większym serwisem lub korzystasz z własnej serwerowni, to wszystkie testy powinny być wykonane w siedzibie firmy. W ten sposób będzie można łatwo sprawdzić nie tylko kondycję strony, ale i zgodność z wytycznymi RODO.

Kluczowa rola backupów i planów awaryjnych

W obliczu nieustannie rosnącego ryzyka cyberataków oraz możliwości wystąpienia awarii technicznych, regularne tworzenie kopii zapasowych danych i opracowanie skutecznych planów awaryjnych jest kluczowe dla zapewnienia ciągłości działania Twojej strony.

Ludzie dzielą się na tych, którzy wykonują kopie bezpieczeństwa i na tych, którzy będą je robić. Backupy pozwalają na szybkie przywrócenie strony internetowej do stanu sprzed incydentu, minimalizując tym samym skutki ataku lub awarii. Kopie zapasowe powinny obejmować zarówno pliki strony, jak i bazy danych.

Małe strony-wizytówki czy blogi mogą zdecydować się na jeden backup dziennie. W przypadku większych projektów lepiej zainwestować w hosting, który wykonuje kopię plików co godzinę. Ważne jest, aby te były przechowywane w bezpiecznej lokalizacji, najlepiej poza główną infrastrukturą, co zapewnia dodatkową ochronę przed atakami typu ransomware.

Oprócz backupów niezwykle ważnym elementem strategii bezpieczeństwa jest opracowanie planu reagowania na incydenty (Incident Response Plan, IRP). Taki dokument powinien określać procedury postępowania w przypadku różnych typów incydentów: od wykrycia ataku, przez analizę i izolację zagrożenia, aż po przywrócenie normalnego funkcjonowania strony.

Ostatnim, ale równie ważnym elementem jest edukacja i szkolenie personelu odpowiedzialnego za bezpieczeństwo strony. Regularne kursy pomagają utrzymać wysoki poziom gotowości do działania. Wiedza i umiejętności pracowników są równie ważne, jak wspomniane wcześniej techniczne środki bezpieczeństwa.

Bez względu na to, czy prowadzisz bloga czy duży sklep online lub portal, który pozwala na tworzenie kont użytkowników i gromadzi o nich wiele danych, musisz zadbać o higienę cyfrową takiego projektu. Dla cyberprzestępców nawet szczątkowe dane są niezwykle cenne.

Zwróć też uwagę na to, że należyta ochrona stron w sieci to nie tylko opcja, ale wręcz obowiązek. Naruszenie wytycznych RODO może kosztować Cię naprawdę sporo. Tylko w 2022 roku z tytułu niewłaściwej ochrony informacji wrażliwych Urząd Ochrony Klienta i Konsumenta nałożył na firmy kary w łącznej kwocie ponad 6 milionów złotych. W 2023 roku, na terenie całej Unii Europejskiej, zasądzono grzywny w kwocie przekraczającej 2 miliardy euro! ●

Czy cyberbezpieczeństwo powinno być jak Yeti?

Krzysztof Szczepański
Dyrektor Departamentu Bezpieczeństwa i Ryzyka w KIR

Pierwotnie bezpieczeństwo IT, na które z czasem przyjęto określenie cyberbezpieczeństwo, skupiało się na ochronie zasobów informatycznych. Ta rola w sposób istotny zmienia się w ostatnich latach. Głównym podmiotem podlegającym ochronie stały się procesy i dane, w tym szczególnie – z coraz większym priorytetem – dane osobowe, które są przetwarzane w systemach. Wydaje się, że historia informatyki wykorzystywanej powszechnie w biznesie jest relatywnie krótka, a jednak ten proces dynamicznie rozwija się już cztery dekady. Obecnie technologie informatyczne są nierozerwalnie związane z gospodarką i prowadzeniem firm.

Technologie informatyczne stosujemy praktycznie w każdym aspekcie naszego życia. Wspierają pracę, rozrywkę, pomagają w codziennym życiu. Coraz więcej czasu spędzamy w cyberprzestrzeni i jesteśmy coraz bardziej zależni od tej aktywności. Nie chodzi tu tylko o wsparcie aktywności biznesowej, ale również o codzienne korzystanie z zasobów informatycznych. Ludzie rzadziej wchodzą w bezpośrednie interakcje i obserwują otoczenie, a coraz szybciej sięgają po telefon w sytuacji, gdy np. czekają na coś. Mamy tendencję do poszukiwania rozwiązań na skróty, stosowania propozycji z sieci jako sposobów na swoje wyzwania, bez refleksji i analizy. Skoro nawigacja pokazuje drogę do celu, to po co się zastanawiać czy jest jakaś lepsza opcja? Zaczynamy ufać technologii bezkrytycznie, bo zwalnia nas ona z myślenia. Dzięki temu mamy więcej czasu i energii na aktywności, które są dla nas ciekawsze. Przestaliśmy też obciążać naszą pamięć, mając dostępne wsparcie narzędzi, które nam przypomną co mamy zrobić. To są naturalne zachowania i od związania ludzi z technologią nie uciekniemy.

Uzależnienie od technologii stało się coraz bardziej powszechne w dzisiejszym społeczeństwie. Przyczyniło się do tego kilka zjawisk. Technologia umożliwia nam komunikację na odległość, zarówno w pracy, jak i w życiu osobistym. Portale społecznościowe, aplikacje do przekazywania wiadomości czy wideokonferencje stały się nieodłączną częścią codzienności. Technologia ułatwia nam życie, dzięki niej możemy załatwiać sprawy online, robić zakupy, płacić rachunki czy zarządzać swoimi finansami. To oszczędza czas i wysiłek. Strumieniowanie muzyki i filmów, gry komputerowe, a nawet monitorowanie zdrowia – to wszystko dostępne jest online dzięki technologii, a współczesne stanowiska pracy i systemy edukacyjne coraz bardziej polegają na technologii.

Trzeba jednak pamiętać, że o umiejętnym korzystaniu z tych współczesnych udogodnień. Dostępna technologia może działać jak narkotyk, wywołując uczucie przyjemności i potrzebę ciągłego korzystania. Uzależnienie od smartfonów czy mediów społecznościowych jest coraz częstsze. Dlatego tak ważne jest, aby zachować równowagę między korzystaniem z nowoczesnych narzędzi a dbaniem o zdrowie psychiczne i fizyczne.

Cyberbezpieczeństwo – czy w ogóle go potrzebujemy?

I tu czas na pytanie, a gdzie w tym wszystkim cyberbezpieczeństwo? I czy w ogóle jest ono nam potrzebne? Dlaczego zadajemy sobie tyle trudu, żeby ograniczać i komplikować korzystanie ze wspaniałych narzędzi cyfrowych? W wielu przedsiębiorstwach funkcjonuje stereotypowe postrzeganie specjalistów od cybersecurity jako osób pozbawionych ▶

poczucia humoru, którzy stale szukają dziury w całym i blokują korzystanie z technologii. Cyberbezpieczeństwo budzi opór i niechęć. Czemu zespoły odpowiedzialne za cyberbezpieczeństwo na siłę chronią i utrudniają ludziom korzystanie z dostępnych funkcjonalności?

Zagadnienia związane z bezpieczeństwem cyfrowym mogą być trudne do przyswojenia dla osób spoza tego obszaru. Samo bezpieczeństwo jest pojęciem dość ulotnym, z zakresem odpowiedzialności często niezrozumiałym dla przeciętnego użytkownika i wymaganiami, które obciążają innych. Nic dziwnego, że ludzie często przedkładają wygodę czy szybkość ponad bezpieczeństwo. W dodatkowych zabezpieczeniach nie widzą bezpośrednich korzyści, a jedynie ograniczenia i utrudnienia. Bywa, że dopiero w przypadku, gdy nastąpi jakiś incydent czy przykre zdarzenie, zaczynają żałować, że nie skorzystali z zaleceń ekspertów od bezpieczeństwa.

Ewolucja zagrożeń

Wirtualna rzeczywistość stała się areną coraz bardziej zaawansowanych ataków cybernetycznych. Skala zagrożeń rośnie, a ich dynamika przyspieszyła, szczególnie w okresie pandemii. Przejście na pracę zdalną i hybrydową otworzyło nowe możliwości dla cyberprzestępców. Obserwujemy coraz więcej ataków bazujących na socjotechnice. Przestępcy wykorzystują ludzką ciekawość, lęki czy chęć zysku, podszywając się pod różne instytucje oraz firmy, wyłudzają dane i prowadzą zaawansowane scenariusze nakłaniające do dysponowania swoim majątkiem w sposób wskazywany przez przestępców.

Jak zmieni się perspektywa zagrożeń w nadchodzącej przyszłości? W ostatnich pięciu latach najistotniejsze zagrożenia to: ataki poprzez malware, w tym ransomware, ataki poprzez strony i aplikacje www, phishing i spam oraz DDoS. Na dalszych pozycjach znajdują się takie zagrożenia jak kradzież tożsamości czy kradzież i wyciek danych. Natomiast w perspektywie nadchodzących lat, biorąc pod uwagę zmiany geopolityczne i nowe scenariusze wojny hybrydowej, oczekujemy rozszerzenia pola walki na cyberprzestrzeń. Najistotniejsze zagrożenia będą płynęły z łańcucha dostaw i zależności od zaawansowanych komponentów technologicznych, wpływu na społeczeństwo poprzez dezinformację i deepfake. Duże znaczenie będzie mieć wzrost incydentów kradzieży tożsamości, utrata prywatności oraz błędy ludzkie i podatności w systemach. Będzie to dotyczyło zwłaszcza urządzeń mobilnych. Obserwujemy postępującą transformację, która ma gwarantować atakującym możliwie najpełniejszy dostęp i wpływ na szerokie grono odbiorców. W rezultacie umożliwi to prowadzenie przestępczych działań z chirurgiczną precyzją. Jednocześnie nie oznacza to ograniczenia zagrożeń związanych z wyłudzeniami czy atakami ransomware. Po prostu, te wskazane wyżej staną się istotniejsze.

Zmieniające się otoczenie, rosnące zagrożenia i nowe regulacje wymuszają bardziej proaktywne podejście do cyberbezpieczeństwa. Warto inwestować w edukację, budowanie świadomości i zaufane technologie, aby skutecznie chronić się przed atakami.

Co – poza przepisami – jest niezbędne by stawić czoła atakom?

Na poziomie regulacyjnym mamy wymagania definiowane przez unijny akt o odporności cybernetycznej (CRA) czy zapisy w dyrektywie NIS2, które wymagają proaktywnego podejścia do bezpieczeństwa, wdrożenia procesów zarządzania ryzykiem i opracowania planów reagowania. Niezależnie jednak od regulacji, każda organizacja i każda osoba, powinna zweryfikować swoje zachowania w cyberprzestrzeni, biorąc pod uwagę ewolucję zagrożeń. Kluczowa jest uważność, ograniczone zaufanie i krytyczna postawa w stosunku do wszelkich informacji - zwłaszcza takich, które powodują chęć wykonania jakiegoś wcześniej nieplanowanego działania lub mających na celu zmianę naszych opinii.

Zmieniające się otoczenie, rosnące zagrożenia i nowe regulacje wymuszają bardziej proaktywne podejście do cyberbezpieczeństwa. Aby skuteczniej chronić się przed atakami warto inwestować w edukację, budowanie świadomości i zaufane technologie. Rosnące wolumeny przetwarzanych informacji zwiększają ekspozycję na ryzyko. Trzeba je poddawać analizie, właściwie oceniać i minimalizować skutki poprzez zastosowanie mechanizmów technologicznych - narzędzi czy środków organizacyjnych opartych na świadomości ludzi korzystających z dobrodziejstw ery cyfrowej.

Cyberbezpieczeństwo – co właściwie chronimy?

W sieci przechowujemy coraz więcej informacji o nas samych, naszych rodzinach, finansach i zdrowiu. Mechanizmy cyberbezpieczeństwa mają chronić nasze dane przed nieuprawnionym dostępem, kradzieżą lub wykorzystaniem w sposób, który może nam zaszkodzić. Widzimy już na przykładach dostępnych w sieci, jak można

zmieniać dostępne publicznie zdjęcia czy nagrania, fałszując zdarzenia i tworząc nieprawdziwe wrażenia u odbiorcy przekazu (tzw. deepfake).
Cyberbezpieczeństwo pomaga aktywnie przeciwdziałać wirtualnym atakom, które wykorzystując schematy ludzkich zachowań, skutkują błędami w dysponowaniu zasobami. Celem przestępców jest kradzież pieniędzy z naszych kont bankowych i wyłudzenia w wyniku wystymulowanej chęci dodatkowego i nieprawdopodobnego zysku. Celowane zabezpieczenia wdrażane są na wielu poziomach, począwszy od zabezpieczenia urządzeń, poprzez stosowanie narzędzi filtrujących i chroniących komunikację elektroniczną, aż do poziomu operatorów telekomunikacyjnych i właściwych CERT-ów poziomu krajowego.

Warto pamiętać, że cyberbezpieczeństwo jest kluczowe dla ochrony naszych danych, finansów i prywatności. Edukacja, świadomość i proaktywne działania mogą pomóc w zminimalizowaniu ryzyka.

Ataki w cyberprzestrzeni mogą powodować ogromne straty finansowe, utratę reputacji i wyciek poufnych informacji. Firmy przechowują dane swoich klientów, pracowników i partnerów biznesowych, a zabezpieczenie ich stanowi kluczowy aspekt działalności i ochrony interesów każdego przedsiębiorcy. Coraz większa świadomość znaczenia cyberbezpieczeństwa, stosowanie zaawansowanych technologii zabezpieczeń, a także wymiana informacji między podmiotami, przyczynia się do wzrostu odporności całych sektorów gospodarki, a w szerszej perspektywie całego społeczeństwa.
Współczesne państwa są coraz bardziej zależne od sprawności infrastruktury cyfrowej. Ataki na systemy krytycznej infrastruktury, takie jak elektrownie, sieci energetyczne czy systemy obronne, mogą mieć poważne konsekwencje dla bezpieczeństwa narodowego. Mogą prowadzić do awarii systemów informatycznych, co zakłóci lub uniemożliwi działanie firm, instytucji publicznych i innych organizacji. Mamy szansę wyciągać wnioski i uczyć się na przykładzie działań w Ukrainie. Informacje te trzeba umiejętnie analizować i odpowiedzialnie wykorzystywać, by zwiększać swoją odporność na zagrożenia - również w perspektywie obrony przed agresją cyfrowych bojówek inspirowanych i utrzymywanych przez wrogie siły. Dbając o bezpieczeństwo usług cyfrowych, minimalizujemy ekspozycję na ryzyko ich wykorzystania ze szkodą dla naszego państwa.
W miarę upowszechniania się technologii, rozwija się również edukacja na temat bezpieczeństwa cyfrowego. Coraz lepiej rozumiemy, że korzystanie z internetu i urządzeń elektronicznych wiąże się z pewnymi ryzykami. Ostrożniej postępujemy z hasłami, częściej wystrzegamy się korzystania z nieznanych źródeł i klikania w podejrzane linki. Organizacje rządowe, instytucje edukacyjne i firmy prowadzą kampanie informacyjne na temat cyberbezpieczeństwa dla swoich klientów i użytkowników. To pomaga podnieść świadomość i zachęca do stosowania dobrych praktyk.
Przemysł 4.0, automatyzacja, sztuczna inteligencja, internet rzeczy (IoT) – to technologie, które rewolucjonizują gospodarkę. Jednak ich adopcja musi iść w parze z cyfrowym bezpieczeństwem. Firmy standardowo inwestują w badania i rozwój, ale muszą planować też odpowiednie środki na obszar cyberbezpieczeństwa. Jest to kluczowe dla zapewnienia zrównoważonego rozwoju społeczeństwa i zachowania zaufania do nowych technologii.
Paradoksalnie wzrost liczby ataków, takich jak ransomware, phishing czy ataki DDoS, odnotowany w mediach sprawia, że rośnie świadomość znaczenia cyberbezpieczeństwa. Mimo tego trudno oczekiwać, abyśmy jako społeczeństwo zdawali sobie sprawę z pełnego zakresu zagrożeń.
Cyberataki mogą się dziać w tle, a ich efekty mogą być odczuwalne dopiero po pewnym czasie. Z zasady są trudne do wykrycia, a ofiary dowiadują się o nich dopiero w momencie, gdy już wyrządzono znaczną szkodę. Takie zdarzenia naruszają zaufanie i prywatność, bezpieczeństwo finansowe, zaburzają funkcjonowanie kluczowych instytucji, destabilizując dostęp do podstawowych dóbr i usług. Dlatego powszechnej edukacji i proaktywnym działaniom musi towarzyszyć stałe, choć często niewidoczne, wsparcie ekspertów od cyberbezpieczeństwa. W tym sensie cyberbezpieczeństwo jest jak Yeti – pozostaje nieuchwytne dla przeciętnego użytkownika. Różnica jest taka, że w cyberbezpieczeństwo trzeba wierzyć, bo zagrożenia istnieją nawet wtedy, kiedy ich nie dostrzegamy, a świadome korzystanie z narzędzi bezpieczeństwa cyfrowego pozwala nas skuteczniej chronić. ●

CO ROBIĆ, ŻEBY BYĆ BEZPIECZNYM

- Aktualizuj oprogramowanie na komputerze
- Zainstaluj program antywirusowy
- Stosuj silne i różne hasła
- Zainstaluj firewall (zaporę sieciową)
- Pobieraj aplikacje tylko z zaufanych źródeł
- Wykonuj kopie zapasowe ważnych danych
- Określ w ustawieniach przeglądarki internetowej, które dane mają być przez nią przechowywane
- Szyfruj dane na dysku komputera i na dyskach zewnętrznych - wtedy nikt niepowołany nie otworzy twoich plików
- Chroń urządzenia przed dostępem niepowołanych osób
- Blokuj telefon i komputer

CZEGO NIE ROBIĆ

- Pamiętaj, że żaden bank ani urząd nie wysyła do swoich klientów e-maili lub smsów z prośbą o podanie hasła lub loginu
- Nie podawaj swoich danych osobowych w niesprawdzonych serwisach i na stronach www
- Nie klikaj w podejrzane linki, np. znajdujące się w odebranej wiadomości lub na portalu społecznościowym
- Nie otwieraj i nie pobieraj plików z niepewnych źródeł
- Nie podłączaj do komputera urządzeń nieznanego pochodzenia
- Nie umieszczaj w sieci informacji, które mogą ci kiedyś zaszkodzić
- Nie obrażaj innych w sieci

Niebezpieczne związki

czyli gangsterzy i filantropi

Michał Jurek
dyrektor Departamentu i Monitorowania Ryzyka i Restrukturyzacji IPS-SGB

Bankowanie w sieci jest dziś oczywiste. Trudno sobie bez niego wyobrazić codzienne funkcjonowanie ludzi i przedsiębiorstw. Ale podobnie oczywiste jest też to, że w ślad za dematerializacją pieniądza i upowszechnieniem płatności bezgotówkowych do sieci przenieśli się również przestępcy.

Nie trzeba już snuć finezyjnych planów napadu na bank, niczym Thomas Crown i jego ekipa, a następnie wywozić zdobytą gotówkę w podróżnym sakwojażu do banku w Szwajcarii. Wystarczy dobry komputer i takież umiejętności, by w krótkim czasie ogołocić konta ofiar z pieniędzy.

Niestety, świadomość istniejących zagrożeń wciąż nie jest wystarczająca. Wskazuje na to choćby Raport Antyfraudowy BIK 2023, zbierający wyniki kilku badań na ten temat, przeprowadzonych w minionym roku. Przez pojęcie fraudu rozumie się w nim każde działanie, w wyniku którego oszust kradnie lub wykorzystuje dane osobowe ofiary w celu przejęcia konta. Co ważne, działanie to nie musi odbywać się tylko i wyłącznie za pośrednictwem sieci internetowej, do czego powrócę jeszcze w dalszej części felietonu.

Niefrasobliwość – grzech główny

Z badań przeprowadzonych przez grupę BIK wyłania się niepokojący obraz. Rośnie bowiem wprawdzie wiedza na temat zagrożeń, ale równie silna jest przy tym wiara badanych, że ich te zagrożenia nie będą dotyczyć. Dlatego też wśród małych i średnich przedsiębiorstw jako główną formę zabezpieczenia wskazuje się własny zdrowy rozsądek. Ponad 82% ankietowanych przedsiębiorców z tej grupy nie korzysta z żadnych usług i narzędzi antyfraudowych. Taka postawa wynika z przekonania, że ryzyka nie są duże, a firmy poradzą sobie z nimi we własnym zakresie.

Dalej – dwie trzecie osób fizycznych ma świadomość tego, że efektem kradzieży danych może być zaciągnięcie kredytu i pożyczki, ale

Najmniej bezpiecznym ogniwem systemu bezpieczeństwa jest człowiek.

zarazem 10% (aż 10%) nie uważa, że wyciek danych osobowych powinien być powodem do niepokoju.

Niefrasobliwość ludzka daje przestępcom wielkie pole do popisu. Nieustannie też ewoluują sposoby, za pomocą których realizują oni swoje niecne zamysły. I tak, według wspomnianego już Raportu Antyfraudowego BIK 2023, przestępcy coraz częściej odcho-

dzą od prób ataków hakerskich na chronione systemy IT instytucji finansowych. Zamiast tego, wykorzystują socjotechnikę tak, by to ofiary skłonić do przeprowadzenia określonych czynności, np. podania danych osobowych i autoryzujących dostęp, zalogowania się na spreparowanej stronie internetowej czy zatwierdzenia zlecenia przelewu na podstawiony przez przestępców rachunek bankowy.

Socjotechnika to sztuka podstępu, jak głosi tytuł książki zmarłego w zeszłym roku Kevina Mitnicka, bodaj najbardziej znanego w latach dziewięćdziesiątych ubiegłego wieku manipulanta i hakera. Jego pomysłowość w nakłanianiu ludzi do udzielania informacji nie miała granic, a że przy tym nerwy miał ze stali i potrafił wychodzić obronną ręką z najcięższych tarapatów, złapany został dopiero w 1995 r. Umieszczono go wówczas w izolatce, ponieważ obawiano się, że gwiżdżąc odpowiednią sekwencję kodu do automatu telefonicznego w więzieniu może nawet wywołać atak nuklearny. Przez wiele lat po opuszczeniu więzienia miał zakaz dotykania komputera.

Ówże Kevin Mitnick stwierdził kiedyś, że łamał ludzi, a nie hasła dostępu, ponieważ najmniej bezpiecznym ogniwem systemu bezpieczeństwa jest właśnie człowiek. Przy czym zaznaczyć należy, że wspomniany Mitnick nie kradł – a przynajmniej nigdy mu tego nie udowodniono. Włamywał się do sieci i dokonywał ataków po prostu dlatego, że mógł.

Niestety, większość przestępców działa w sposób dalece bardziej przyziemny. Nie chodzi im o testowanie systemu zabezpieczeń i wynajdowanie luk, a o kradzież pieniędzy. Brak odpowiedniej świadomości zagrożeń po drugiej, jasnej stronie mocy jest więc niepokojący. Tymczasem BIK wskazuje na systematyczny rozwój stosowanych socjotechnik. W 2023 r. najczęstszym atakiem tego typu był vishing (voice phishing), polegający na wyłudzaniu danych przez telefon poprzez podszywanie się pod jakąś instytucję.

Banki, jako instytucje zaufania publicznego, odpowiadają za bezpieczeństwo swoich klientów. Jednak, by móc skutecznie odpierać ataki cyberprzestępców, niezbędna jest też edukacja samych klientów.

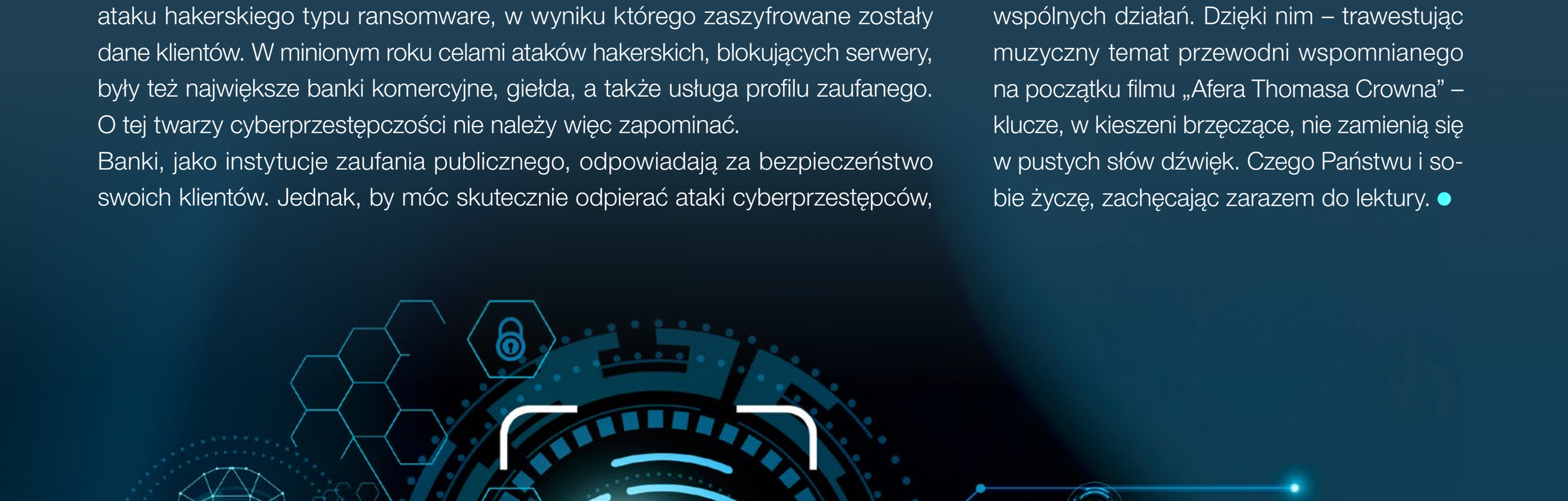
Edukacja, edukacja i... edukacja!

Nie oznacza to jednak, że hakerskie syndykaty nie dokonują już ataków, co to, to nie. Wszak dopiero co jeden z banków spółdzielczych doświadczył poważnego ataku hakerskiego typu ransomware, w wyniku którego zaszyfrowane zostały dane klientów. W minionym roku celami ataków hakerskich, blokujących serwery, były też największe banki komercyjne, giełda, a także usługa profilu zaufanego. O tej twarzy cyberprzestępczości nie należy więc zapominać.

Banki, jako instytucje zaufania publicznego, odpowiadają za bezpieczeństwo swoich klientów. Jednak, by móc skutecznie odpierać ataki cyberprzestępców, niezbędna jest też edukacja samych klientów. Jak podkreśla BIK, trzeba nieustanie, wręcz do znudzenia, przypominać klientom, że pracownik banku nigdy nie prosi przez telefon o podanie danych osobowych, że nie należy otwierać przesłanych w mailach i SMS-ach linków lub załączników bez zweryfikowania nadawcy, a wreszcie – że należy stosować odpowiednio bezpieczne hasła dostępu i je aktualizować, podobnie jak zainstalowany program antywirusowy.

A już za progiem stoją nowe wyzwania i zagrożenia, między innymi rozwój sztucznej inteligencji i technik z zakresu deepfake, wykorzystywanych w coraz bardziej powszechnych oszukańczych reklamach, umieszczanych w serwisach społecznościowych. By tym wyzwaniom sprostać, w zakresie cyberprzestępczości niezbędna jest edukacja, edukacja i jeszcze raz edukacja. Tylko wtedy możliwe będzie skuteczne zapewnienie bezpieczeństwa klientom i zarazem ochrona reputacji instytucji, które oferują im swoje usługi, nie tylko finansowe.

Dla osiągniecia tych celów w sektorze banków spółdzielczych niezbędna jest też współpraca z bankami zrzeszającymi i instytucjonalnymi systemami ochrony. Bankom spółdzielczym trudno będzie samodzielnie zadbać o pełne bezpieczeństwo ich infrastruktury IT, zwłaszcza że nowe regulacje (np. DORA), w sposób znaczny zwiększą zakres odpowiedzialności oraz obowiązków instytucji finansowych w tym zakresie. Ale przecież w jedności siła, czego niejednokrotnie dowiodły już wspólne działania środowiska banków spółdzielczych. Zamieszczone w niniejszym e-wydaniu „Banku Spółdzielczego" artykuły poświęcone kwestii cyberbezpieczeństwa i technologii stanowią dobrą inspirację do takich właśnie wspólnych działań. Dzięki nim – trawestując muzyczny temat przewodni wspomnianego na początku filmu „Afera Thomasa Crowna" – klucze, w kieszeni brzęczące, nie zamienią się w pustych słów dźwięk. Czego Państwu i sobie życzę, zachęcając zarazem do lektury. ●



Łowcy kodów

Jak cybernetyczni złodzieje zagrażają bezpieczeństwu danych

Andrzej Borowiak
rzecznik prasowy Komendanta Wojewódzkiego Policji w Poznaniu

W erze cyfrowego przełomu, kiedy technologia przekształca nasze życie i działalność gospodarczą na skalę niespotykaną dotąd, cyberprzestępczość wyłania się jako jedno z największych wyzwań naszych czasów. Hakerzy, cybernetyczni przestępcy, działają z zamiarem kradzieży danych, szpiegostwa przemysłowego, wymuszeń finansowych i zakłócania normalnego funkcjonowania systemów komputerowych. Ich metody ewoluują, stając się coraz bardziej wyrafinowane i trudne do wykrycia. W tym artykule przyjrzymy się, jak współcześni hakerzy działają oraz jak można się przed nimi obronić.

Jak działa współczesna cyberprzestępczość?

Cyberprzestępcy posługują się różnorodnymi metodami, aby osiągnąć swoje cele. Jedną z najpopularniejszych technik jest phishing, czyli wyłudzanie poufnych informacji poprzez podszywanie się pod zaufane instytucje czy osoby. Przesyłają fałszywe e-maile, sms-y lub używają fałszywych stron internetowych, aby nakłonić ludzi do podania swoich danych osobowych, takich jak hasła czy numery kart kredytowych. Inną powszechną techniką jest atak z użyciem złośliwego oprogramowania, czyli malware. Może to być wirus komputerowy, który infekuje system i szkodzi mu lub ransomware, który blokuje dostęp do danych i wymusza okup w zamian za ich odblokowanie. Ponadto, hakerzy mogą wykorzystywać tzw. ataki typu DDoS (rozproszone ataki odmowy usługi), aby przeładować serwery i uniemożliwić dostęp do danej strony internetowej czy usługi.

Jeden z najbardziej znanych i wpływowych ataków cybernetycznych w historii miał miejsce w 2017 roku i nosi nazwę WannaCry.

Warto również wspomnieć o tzw. social engineering, czyli technikach manipulacji psychologicznej, których celem jest uzyskanie poufnych informacji od ludzi poprzez wykorzystanie ich naiwności, zaufania lub nieuwagi.

Jak uchronić się przed cyberprzestępcami?

Obrona przed cyberprzestępcami wymaga nie tylko stosowania odpowiednich narzędzi i technologii, ale także podniesienia świadomości użytkowników o zagrożeniach oraz odpowiedniego wychowania cyfrowego.

1. Zabezpiecz swoje hasła: Stosuj silne, unikalne hasła do wszystkich swoich kont online i regularnie je zmieniaj. Wykorzystuj również mechanizmy autoryzacji dwuetapowej, które dodatkowo zabezpieczają Twoje konto.
2. Uważaj na phishing: Bądź ostrożny wobec podejrzanych e-maili, wiadomości sms oraz linków i załączników pochodzących z nieznanych źródeł. Nie podawaj swoich danych osobowych ani poufnych informacji bez upewnienia się, że komunikujesz się z zaufaną osobą czy instytucją.
3. Aktualizuj oprogramowanie: Regularnie aktualizuj oprogramowanie swojego systemu operacyjnego oraz aplikacji, aby zapewnić sobie ochronę przed lukami bezpieczeństwa, które mogą być wykorzystane przez hakerów.
4. Zainstaluj antywirus i oprogramowanie anty-malware: Używaj renomowanych programów antywirusowych i anty-malware, które skanują Twoje urządzenie w poszukiwaniu złośliwego oprogramowania i chronią Cię przed atakami.
5. Zabezpiecz swoje sieci Wi-Fi: Używaj silnych haseł do swojej sieci Wi-Fi i unikaj łączenia się z publicznymi sieciami, które mogą być łatwym celem dla hakerów.
6. Bądź ostrożny w mediach społecznościowych: Ogranicz udostępnianie swoich danych osobowych w mediach społecznościowych i uważaj na podejrzane kontakty i wiadomości.
7. Edukacja cyfrowa: Wdrażaj programy edukacyjne dotyczące cyberbezpieczeństwa w swojej organizacji czy instytucji. Ucz swoich pracowników, jak rozpoznawać i reagować na potencjalne zagrożenia.

Jeden z najbardziej znanych i wpływowych ataków

cybernetycznych w historii miał miejsce w 2017 roku i nosi nazwę WannaCry. Atak ten był typowym przykładem ransomware'u, czyli złośliwego oprogramowania, które szyfruje pliki na zainfekowanym komputerze i żąda okupu w zamian za ich odblokowanie. WannaCry wywołał panikę na całym świecie, sparaliżował wiele firm i instytucji oraz spowodował znaczne straty finansowe.

Atak WannaCry rozpoczął się 12 maja 2017

roku, kiedy to brytyjski National Health Service (NHS), system publicznej służby zdrowia w Wielkiej Brytanii, został zaatakowany. Zainfekowane zostały tysiące komputerów w różnych szpitalach i placówkach medycznych, co spowodowało zakłócenia w świadczeniu opieki zdrowotnej dla pacjentów. Szpitale były zmuszone do odwoływania operacji, a personel musiał przeprowadzać procedury ręcznie, ponieważ systemy komputerowe były niedostępne.

WannaCry wykorzystywał lukę w systemie operacyjnym Windows, która została wcześniej wykradziona z Agencji Bezpieczeństwa Narodowego Stanów Zjednoczonych (NSA) i ujawniona przez grupę hakerską o nazwie Shadow Brokers. Atakujący wykorzystali tę lukę, aby rozprzestrzenić się po sieciach komputerowych, szyfrując pliki na zainfekowanych maszynach i żądając od ofiar okupu w kryptowalucie Bitcoin.

Szybkie rozprzestrzenianie się WannaCry wynikało z jego zdolności do samonaprawiania się i infekowania innych komputerów w sieci lokalnej. Zainfekowane maszyny wysyłały złośliwe wiadomości do innych urządzeń w sieci, co prowadziło do lawinowego rozprzestrzeniania się ransomware'u w niezwykle szybkim tempie.

Atak WannaCry wywołał falę reakcji na całym świecie. Firmy, instytucje rządowe i jednostki odpowiedzialne za bezpieczeństwo cyfrowe były zmuszone do natychmiastowych działań w celu zabezpieczenia swoich systemów przed podobnymi atakami. Microsoft wydał natychmiastową łatkę, aby załatać lukę w systemie Windows, którą wykorzystywał WannaCry, i apelował do użytkowników o aktualizację swoich systemów.

Chociaż atak WannaCry wywołał ogromne szkody i spowodował zamieszanie na całym świecie, przyniósł również ze sobą ważne wnioski. Pokazał, jak istotne jest regularne aktualizowanie systemów operacyjnych i oprogramowania oraz stosowanie zabezpieczeń przeciwko ransomware'owi. Wydarzenie to podkreśliło również potrzebę współpracy międzynarodowej w walce z cyberprzestępczością oraz rozwijania świadomości cyfrowej społeczeństwa, aby chronić się przed podobnymi zagrożeniami w przyszłości.

Jednym z bardziej zauważalnych cyberataków w Polsce

w ostatnich latach był atak na Narodowy Fundusz Zdrowia w maju 2019 roku. NFZ stał się celem ataku hakerskiego, który spowodował zakłócenia w funkcjonowaniu systemów informatycznych tej instytucji. Atak polegał na zainfekowaniu systemu NFZ przez złośliwe oprogramowanie, które zakłóciło pracę sieci komputerowej oraz dostęp do danych i aplikacji NFZ. Skutkiem tego było utrudnione korzystanie z usług NFZ przez pacjentów, a także problemy w pracy personelu medycznego.

W wyniku ataku wielu pacjentów miało utrudniony dostęp do niezbędnych usług zdrowotnych, a pracownicy służby zdrowia musieli radzić sobie z ograniczeniami w dostępie do danych medycznych.

Atak na NFZ wywołał obawy dotyczące bezpieczeństwa danych medycznych oraz podkreślił konieczność podjęcia działań w celu wzmocnienia cyberbezpieczeństwa w sektorze opieki zdrowotnej w Polsce. Incydent ten również zwrócił uwagę na potrzebę inwestowania w lepsze zabezpieczenia systemów informatycznych oraz zwiększenie świadomości w zakresie cyberbezpieczeństwa wśród personelu medycznego i pracowników sektora publicznego.

Atak na NFZ jest jednym z wielu przykładów cyberzagrożeń, z którymi muszą zmierzyć się instytucje i przedsiębiorstwa w Polsce. Podkreśla on również znaczenie ciągłego monitorowania, aktualizacji i wzmocnienia zabezpieczeń informatycznych, aby chronić wrażliwe dane oraz zapobiegać zakłóceniom w działaniu kluczowych instytucji i usług publicznych.

Jednym z najbardziej znamienitych ataków na system bankowy w ostatnich latach był incydent z 2016 roku, który miał miejsce w Bangladeszu. Atak ten był próbą kradzieży ogromnej sumy pieniędzy z banku centralnego tego kraju i stanowił przykład zaawansowanego ataku hakerskiego na infrastrukturę finansową.

W lutym 2016 roku grupa hakerów przeprowadziła atak na system bankowy Bangladeszu, wykorzystując lukę w zabezpieczeniach banku centralnego. Atak opierał się na technice znanej jako SWIFT (Society for Worldwide Interbank Financial Telecommunication), która jest międzynarodowym systemem komunikacji i przekazywania pieniędzy między bankami na całym świecie. Hakerzy uzyskali dostęp do systemu SWIFT i zainicjowali fałszywe transakcje pieniężne na ogromną skalę.

Cyberprzestępcy posługują się różnorodnymi technikami, aby osiągnąć swoje cele. Jedną z najpopularniejszych jest phishing, czyli wyłudzanie poufnych informacji poprzez podszywanie się pod zaufane instytucje.

Atakujący próbowali przelać ponad 1 miliard dolarów z konta banku centralnego Bangladeszu do różnych banków na całym świecie. Choć większość transakcji została zatrzymana przez banki docelowe ze względu na podejrzane czynności, udało się przelać około 81 milionów dolarów na konto w jednym z banków na Filipinach. Jednakże, dzięki szybkiej reakcji banku centralnego Bangladeszu oraz ścisłej współpracy z bankami i organami ścigania na całym świecie, większość skradzionych środków została odzyskana.

Atak na bank centralny Bangladeszu był nie tylko jednym z największych w historii, ale także podkreślił poważne luki w bezpieczeństwie systemów bankowych na całym świecie. Wydarzenie to zmusiło banki do przeglądu swoich procedur bezpieczeństwa, zwiększenia kontroli i monitorowania transakcji oraz inwestowania w bardziej zaawansowane systemy ochrony przed atakami hakerskimi.

Podsumowując, współczesna cyberprzestępczość stanowi poważne wyzwanie dla nas wszystkich. Jednakże, stosując odpowiednie środki ostrożności i dbając o świadomość cyfrową, możemy znacznie zwiększyć nasze szanse na obronę przed atakami hakerów. Pamiętajmy, że nasze działania w zakresie ochrony danych mają kluczowe znaczenie dla bezpieczeństwa naszych informacji i prywatności online. ●

Jak (nie) zostałem **oszukany**

Maciej Karwowski
SGB-Bank SA

Niby wszyscy zdajemy sobie sprawę z wielu czyhających na nas zagrożeń i zdarza nam się nawet podśmiechiwać z bohaterów artykułów pokroju „Podawał się za Willa Smitha. Wyłudził od kobiety 45 tys. złotych”, ale prawda jest taka, że zostanie ofiarą jakiegoś mniej lub bardziej wyrafinowanego przekrętu może zdarzyć się każdemu z nas. Myślicie, że to niemożliwe? Też tak myślałem. Do czasu.

Kilka lat temu wynajmowałem pokój

w mieszkaniu na osiedlu Tysiąclecia w Poznaniu. Pozostałe dwa pomieszczenia zajmowali obcokrajowcy, dlatego wszelkimi rachunkami zarządzałem ja. Część dostawaliśmy listownie, o części informacja szła od właścicielki. I ten system działał bez zarzutu.

Pamiętny piątkowy wieczór spędzałem typowo dla siebie w kinie. Seans kilkukrotnie zakłócił mi wibrujący telefon. Gdy wyszedłem z pokazu, sprawdziłem kto dzwonił – miałem dwa nieodebrane połączenia oraz dwa SMS-y od właścicielki mieszkania. W pierwszym informowała o niedopłacie za gaz; drugi, wysłany po ledwie kilku minutach, opatrzony kilkoma wykrzyknikami stanowił ponaglenie o konieczności uregulowania tej należności. Pierwsza wiadomość straszyła wizją odcięcia usługi, jeśli przelew nie zostanie wysłany do jutra. A był to przecież początek weekendu, więc poczułem presję szybkiego działania. Kwota opiewała na ledwie kilka złotych, temat nie wydawał się trudny do rozwiązania. Odruchowo kliknąłem w znajdujący się w SMS-ie link.

Na stronie opatrzonej logotypem dostawcy usługi wpisałem swoje dane bankowe. I dopiero kliknąwszy „Enter” zamarłem, uświadamiając sobie, że przecież nie tak cały ten proces powinien wyglądać. Skąd niby nagle pojawiła się niedopłata? Dlaczego dostawca gazu miałby nie dawać czasu na

> Scamerzy doskonale znają nasze słabości i wciąż będą próbowali je wykorzystywać, na coraz bardziej wymyślne sposoby.

przeanalizowanie sytuacji? Dlaczego miałbym logować się do swojego konta przez jakąś stronę? Pytania w głowie zaczęły się mnożyć wespół z kroplami potu na czole. Szybki telefon do banku, blokada wszystkiego, czego się da. Niestety było już o kilka sekund za późno – z konta zniknęło 2800 zł.

Na nic zdała się wizyta w banku czy na policji – takie działania są trudne do wykrycia, a na odzyskanie pieniędzy przecież nie ma co liczyć, skoro sam dałem przestępcom dostęp do konta! Trzeba było przełknąć tę gorzką pigułkę (oczywiście czerwoną) i w ten sposób zapłacić za swoją głupotę. Szkoda jedynie, że do odpowiedzialności nie poczuła się właścicielka mieszkania, która bezmyślnie przekopiowała fishingową wiadomość, będąc jej oryginalną adresatką. Ale może nie powinienem stosować tak oceniającego tonu, skoro to ja dałem się naciąć na dość oczywisty przekręt.

Fatalny telefon od mamy

Druga historia pojawiła się w moim życiu poprzez telefon od mamy. Kobieta rocznik ’61, z internetu korzystająca głównie do oglądania filmów oraz kupowania/sprzedawania drobiazgów. Siłą rzeczy jestem dla niej „młodszym specjalistą ds. komputerowych” i raz na jakiś czas dzwoni, by o coś dopytać. Tym razem bardzo zdawkowo poinformowała mnie, że robi transakcję w internecie i że z jakiegoś powodu karta nie chce przejść, więc czy mogłaby użyć mojej. Nie wnikając podałem jej dane, wraz z kodem CVC i się pożegnaliśmy. Po chwili odezwała się ponownie, mówiąc że problem nie ustał i dopiero wtedy wyjaśniła mi o co dokładnie chodzi.

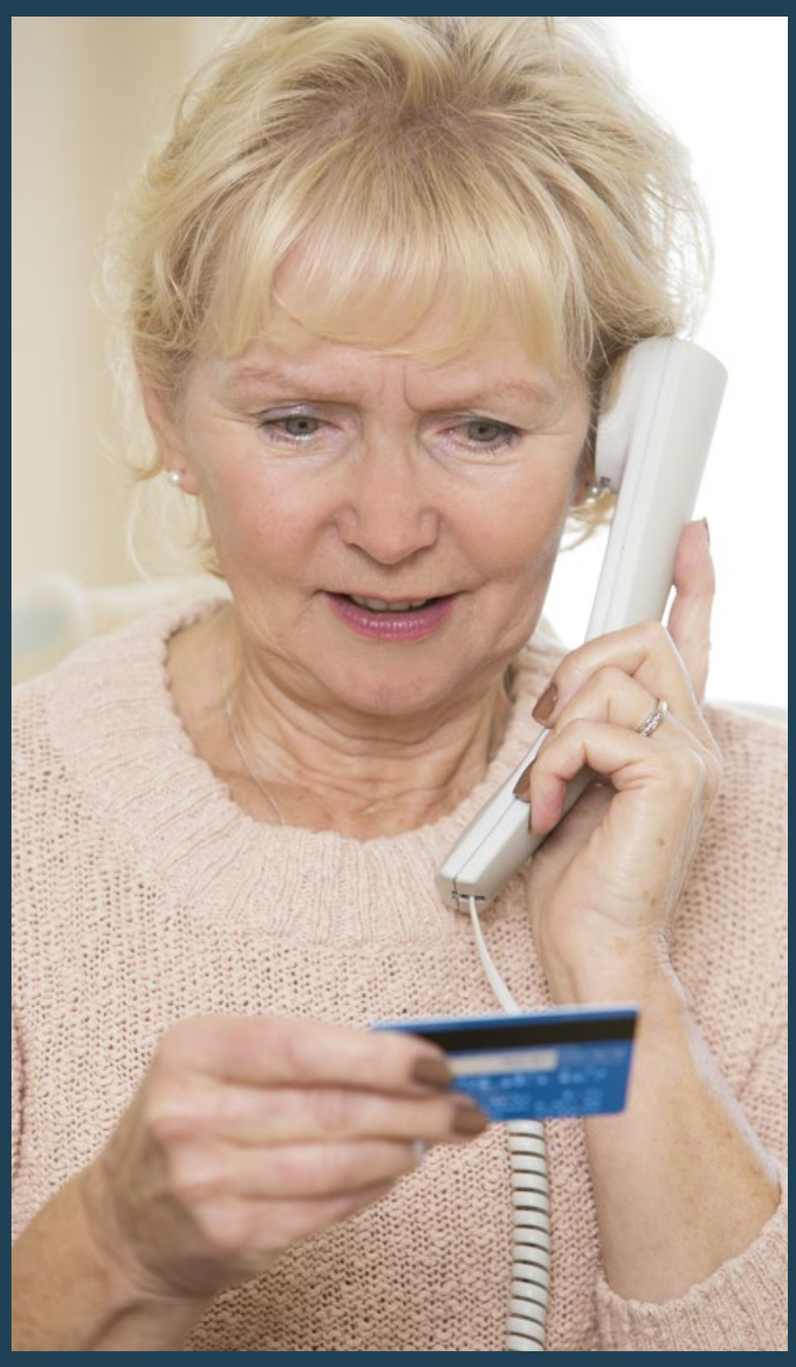
Otóż wystawiła na aukcję jakieś ubranie i ktoś odezwał się do niej na WhatsAppie. Tajemniczy jegomość napisał, że już zamówił kuriera i tylko trzeba coś potwierdzić, rzecz jasna poprzez kliknięcie w link i podanie danych karty. Nie zapaliła jej się lampka ostrzegawcza, z takim działaniem spotkała się pierwszy raz w życiu.

A gdy transakcji nie udało się sfinalizować, wciąż nie wyczuwając potencjalnego przekrętu, chciała spróbować z inną kartą. Dopiero rozmawiając ze mną uświadomiła sobie, że przecież sprzedając przedmiot to nie ona powinna podawać numer karty na jakimkolwiek etapie transakcji. Na całe szczęście przekazując oszustowi moją kartę, wciąż podawała swoje dane, dlatego u mnie żadnych prób wyprowadzenia pieniędzy nie odnotowaliśmy.

Natomiast z konta mamy próbowano natychmiastowo przelać kilka tysięcy złotych. Transakcje zostały zablokowane.

Czemu? Ona twierdzi, że ze względu na podanie przez nią pojedynczego nazwiska, podczas gdy wszędzie w dokumentach figuruje pod podwójnym.

Czy faktycznie to zadecydowało – nie wiem, wolę skupić się na poczuciu ulgi, że nic złego finalnie się nie stało. A poskutkowało tym, że mama dzwoni do mnie jeszcze częściej, by upewnić się co do każdego nowego działania, jakie podejmuje w sieci.



Pytania w głowie zaczęły się mnożyć wespół z kroplami potu na czole. Szybki telefon do banku, blokada wszystkiego, czego się da. Niestety było już o kilka sekund za późno – z konta zniknęło 2800 zł.

Z dzisiejszej perspektywy powyższe sytuacje

wydają mi się absurdalne i oczywiste w ocenie. Zwłaszcza, że przecież pracuję w banku! Po serii szkoleń moja świadomość zagrożeń jest dziś znacznie wyższa. Ale wówczas zadziałało zamroczenie – zaufanie do drugiej osoby, presja czasu i chęć szybkiego załatwienia potencjalnie błahej sprawy. Scamerzy doskonale znają nasze słabości i wciąż będą próbowali je wykorzystywać, na coraz bardziej wymyślne sposoby.

Dlatego nie możemy tracić czujności, niezależnie czego sprawa dotyczy i kto się do nas zwraca. Bo chwila nieuwagi i może być za późno. ●

Judyta Pawłowska
radca prawny
w SGB-Banku SA

Każdy może paść ofiarą cyberprzestępców, to prawda. Równie ważne, co wiedza o możliwych zagrożeniach jest także świadomość tego, co zrobić, by się zabezpieczyć lub możliwie najbardziej zminimalizować szkody. Ważne, by zareagować szybko. Jeśli pokrzywdzony podał przestępcom swoje dane do logowania do bankowości internetowej czy mobilnej, możliwie jak najszybciej powinien ten fakt zgłosić w swoim banku i zablokować dostępy do kanałów elektronicznych. W przypadku karty, należy postąpić podobnie i niezwłocznie ją zastrzec. To uniemożliwi przestępcom dalsze działania.

Oczywiście, ważne jest by takie sytuacje zgłaszać niezwłocznie organom ścigania.

Jeżeli przestępca wszedł w posiadanie naszych dokumentów tożsamości lub danych umożliwiających uzyskanie pożyczki również i ten fakt należy zgłosić organom ścigania oraz uzyskać zaświadczenie o złożeniu zawiadomienia o możliwości popełnienia przestępstwa kradzieży dokumentu tożsamości czy danych osobowych. Będzie to pomocne w razie ewentualnych działań windykacyjnych podejmowanych przez podmioty, u których zostały zawarte umowy pożyczek na skradzione dane.

Nowym i pomocnym narzędziem jest także możliwość zastrzeżenia numeru PESEL przez internet lub w urzędzie.

Dla tzw. świętego spokoju polecam także ustawienie dla siebie alertów o ewentualnych pożyczkach/kredytach.

Obowiązki banku w sytuacji wykorzystywania jego działalności do działań przestępczych

Judyta Pawłowska
SGB-Bank SA

Zakładanie rachunków na tzw. „słupy", wyłudzanie kredytu, fałszywe inwestycje czy kradzież środków klienta w związku z włamaniem na jego konto to tylko niektóre przykłady przestępstw popełnianych przy wykorzystaniu działalności banków.

Mimo dość dużej świadomości społeczeństwa na ten temat, nadal mamy do czynienia ze sporym odsetkiem popełnianych przestępstw przy wykorzystaniu działalności bankowej na szkodę klientów banków, a także i samych banków. W określonych przypadkach skutkować to powinno złożeniem przez bank zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa.

> Ujawniane informacje przez bank powinny jednak mieć bezpośredni związek z przestępstwem, o którym bank zawiadamia właściwy organ.

Obowiązek powiadomienia właściwych organów ścigania o uzasadnionym podejrzeniu popełnienia przestępstwa został wprowadzony do Prawa bankowego w 2004 r. Zgodnie z art. 106a ust. 1 Pr. bankowego:

"W razie zaistnienia uzasadnionego podejrzenia, że działalność banku jest wykorzystywana w celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem skarbowym lub innym przestępstwem niż przestępstwo, o którym mowa w art. 165a lub art. 299 Kodeksu karnego - bank zawiadamia o tym prokuratora, policję albo inny właściwy organ uprawniony do prowadzenia postępowania przygotowawczego."

Powyższy przepis ma na celu ochronę całego systemu bankowego przed wykorzystywaniem go do działalności przestępczej oraz zwiększenie pewności obrotu finansowego, co w dalszej kolejności przekładać się powinno także na zwiększenie zaufania społeczeństwa do sektora bankowego.

Odnosząc się do ww. przepisu, w pierwszej kolejności wskazać należy, że złożenie zawiadomienia ma charakter obligatoryjny, o czym świadczy posłużenie się przed ustawodawcę zwrotem „bank zawiadamia (…)". Wobec czego, każdorazowo w sytuacji, gdy ziszczą się przesłanki tam opisane, bank powinien zawiadomić o tym fakcie organy uprawnione do prowadzenia postępowania przygotowawczego (np. prokuratora).

Uzasadnione podejrzenie popełnienia przestępstwa

Pierwszą przesłanką zawartą w ww. przepisie jest wystąpienie uzasadnionego podejrzenia, że działalność banku jest wykorzystywana do działań przestępczych (lub do ich ukrycia). W obowiązujących przepisach prawa próżno szukać legalnej definicji uzasadnionego podejrzenia popełnienia przestępstwa. Nie ma bowiem realnej możliwości ustalenia tego pojęcia chociażby z uwagi na wielość przestępstw oraz sposobów ich popełniania, czy to, że samo podejrzenie jest elementem subiektywnym, które jest dopiero oceniane na podstawie racjonalnych kryteriów.

Z wypracowanego w doktrynie i judykaturze stanowiska wynika jednak, że banki powinny stosować podwyższony miernik staranności w takich przypadkach, w szczególności gdy ▸

jednocześnie ujawniają tajemnicę bankową. Powyższe wynika między innymi z faktu, że banki dysponują odpowiednimi narzędziami analitycznymi, posiadają szeroki dostęp do informacji, jak i wysoki poziom wiedzy specjalistycznej. Wobec czego, ustalając, czy w danym przypadku mogło dojść do popełnienia przestępstwa bank powinien dokonać analizy posiadanych przez siebie dokumentów oraz informacji, a następnie ocenić je stosując obiektywne i racjonalne kryteria, a także zasady logicznego rozumowania oraz dotychczasowe doświadczenie.

Przestępstwa przy wykorzystaniu działalności banku

Drugą przesłanką, o której mówi art. 106a ust. 1 Pr. bankowego jest wykorzystanie do działań przestępczych działalności danego banku. Pod pojęciem tym należy rozumieć wszelkiego rodzaju przestępstwa, które są popełniane przy wykorzystaniu działalności bankowej (np. wyłudzenie kredytu, wykorzystywanie rachunku do oszustw inwestycyjnych czy kradzież pieniędzy z rachunku). Obowiązek złożenia zawiadomienia, o którym mowa w art. 106a Pr. bankowego nie powstaje więc w sytuacji powzięcia przez pracowników banku informacji o przestępstwie, które nie zostało objęte ww. przepisem, tj. nie polega w żadnym zakresie na wykorzystaniu działalności banku do działań przestępczych lub do ich ukrycia. W takim przypadku możemy mieć do czynienia np. ze społecznym obowiązkiem złożenia zawiadomienia o możliwości popełnienia przestępstwa (art. 304 Kodeksu postępowania karnego). Obowiązek złożenia zawiadomienia obciąża ten bank, którego działalność została wykorzystana do działalności przestępczej (lub do jej ukrycia).

Z zakresu tego przepisu, ustawodawca wprost wyłączył także przestępstwo prania pieniędzy oraz przestępstwo finansowania terroryzmu odsyłając w tym przedmiocie do trybu opisanego w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Tajemnica bankowa w zawiadomieniu o możliwości popełnienia przestępstwa

Tajemnica bankowa stanowi informację prawnie chronioną. Jej ujawnienie może odbywać się jedynie w przypadkach opisanych w obowiązujących przepisach prawa. Choć przepis art. 106a Pr. bankowego wprost nie wskazuje na możliwość ujawnienia tajemnicy bankowej w toku składania zawiadomienia o możliwości popełnienia przestępstwa, to należy uznać, że uprawnienie to wynika z samej wykładni celowościowej ww. przepisu. Potwierdza to ugruntowane w tym zakresie stanowisko doktryny i orzecznictwa. Bank ma więc prawo do ujawnienia tajemnicy bankowej w związku ze składanym przez siebie zawiadomieniem o możliwości popełnienia przestępstwa (a także następnie w toku uzupełniania tego zawiadomienia).

Należy zauważyć bowiem, że obowiązek zawiadamiania przez banki organów ścigania o popełnianych przestępstwach został wprowadzony między innymi po to, by usprawnić i znacznie przyspieszyć proces ścigania sprawców takich przestępstw. Ujawniane informacje przez bank powinny jednak mieć bezpośredni związek z przestępstwem, o którym bank zawiadamia właściwy organ. W piśmiennictwie wskazuje się, że ustalając zakres udostępnianych danych, bank nie powinien wykroczyć poza zakres określony w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Przekroczenie przez bank dozwolonego zakresu udostępnianych informacji w związku ze składanym zawiadomieniem o możliwości popełnienia przestępstwa może zostać uznane za naruszenie ustawowego obowiązku zachowania tajemnicy bankowej i w konsekwencji może spotkać się z nałożeniem sankcji.

Zakładanie rachunków na tzw. „słupy”, wyłudzanie kredytu, fałszywe inwestycje, czy kradzież środków klienta w związku z włamaniem na jego konto to tylko niektóre przykłady przestępstw popełnianych przy wykorzystaniu działalności banków.

Realizacja obowiązku złożenia zawiadomienia przez bank

Bez względu na wynik postępowania karnego, bank nie ponosi odpowiedzialności odszkodowawczej w przypadku, gdy dochował należytej dla siebie staranności przy realizacji obowiązku złożenia zawiadomienia o możliwości popełnienia przestępstwa, w tym także z tytułu zastosowanej przez siebie blokady środków. ●

SALTUS UBEZPIECZENIA

saltus.pl

Nowe ubezpieczenie mieszkań i domów jednorodzinnych SALTUS – Mój DOM

W obliczu dynamicznie zmieniających się potrzeb i oczekiwań klientów nieustannie dążymy do innowacji oraz rozwijania naszej oferty, aby zapewnić najwyższy poziom zabezpieczenia dla klientów Banków Spółdzielczych. Z wielką przyjemnością informujemy o wprowadzeniu na rynek naszego najnowszego produktu: **ubezpieczenia mieszkań i domów SALTUS – Mój DOM**, które zostało zaprojektowane z myślą o zapewnieniu kompleksowej ochrony najcenniejszego majątku i mienia klientów.

Statystyki i potrzeby

Badania PIU/Millman z 2022 roku wskazują, że **aż 60% Polaków** zabezpieczyło już swoje domy i mieszkania. Nasza nowa oferta stanowi odpowiedź na rosnącą świadomość i potrzebę ochrony majątku wśród naszych rodaków.

Ubezpieczenie to wydatek. Wystarczy jednak policzyć, żeby przekonać się, że zwykle mniejszy niż nasze standardowe wydatki.

Typowe wydatki domowe w ciągu roku:
Rachunek za telefon – 1300 zł
Abonament za serwisy filmowe – 780 zł
Siłownia, joga – 1400 zł
Internet i kablówka – 1320 zł
Ubezpieczenie mieszkania – 557 zł
Od wszystkich ryzyk dla mieszkania wartego 410 000 zł i ruchomości domowych wartych 30 000 zł, także od kradzieży.

Ubezpiecz to, co się liczy!

SALTUS - Mój DOM
UBEZPIECZENIE MIESZKAŃ I DOMÓW JEDNORODZINNYCH

Czym wyróżnia się nowe ubezpieczenie?

Ubezpieczenie SALTUS – Mój DOM zostało zaprojektowane z myślą o zapewnieniu maksymalnej ochrony dla najcenniejszych aktywów klientów, jakim są mieszkanie lub dom. Umożliwia ono ubezpieczenie nie tylko tradycyjnych elementów takich jak mieszkanie, dom jednorodzinny, czy ruchomości domowe, ale również oferuje ochronę dla nowoczesnych rozwiązań, takich jak panele fotowoltaiczne czy drobny sprzęt medyczny. Nowością są także opcje zabezpieczenia roślin i akcesoriów ogrodowych, co jest odpowiedzią na coraz większe zainteresowanie klientów takim rozwiązaniem.

Zakres ochrony

Klient decydując się na ubezpieczenie od **SALTUS Ubezpieczenia**, może wybrać ochronę przed szerokim wachlarzem ryzyk - począwszy od pożaru, poprzez powódź, aż po kradzież z włamaniem. Co więcej, wprowadziliśmy opcję ubezpieczenia **All Risk, oznaczającą ochronę od wszystkich szkód**, co jest znaczącym udogodnieniem, na które często decydują się klienci.

Dodatkowe opcje

Oprócz standardowego zakresu ubezpieczenia, nasi klienci mogą również skorzystać z dodatkowych opcji, takich jak **ubezpieczenie NNW**, **medical assistance**, **ubezpieczenie OC** oraz **Assistance Mój DOM**, oferujące pomoc w nagłych sytuacjach domowych. Nowością jest również ubezpieczenie wyłudzenia gotówki będące odpowiedzią na rosnące ryzyko tzw. „wyłudzeń na wnuczka".

SALTUS UBEZPIECZENIA

saltus.pl

Współpraca z SALTUS Ubezpieczenia

Zrzeszenie SGB, w drugiej połowie roku 2023, podpisało umowę o współpracy z SALTUS Ubezpieczenia.

Wiele Banków Spółdzielczych ze Zrzeszenia SGB już od 2021 roku współpracuje z SALTUS Ubezpieczenia, a kolejne sukcesywnie dołączają do tego grona – na koniec 2023 roku były to już **24 banki**. Był to zdecydowanie dobry ruch biznesowy dla obu stron – nasze inkaso, a więc i przychód banków z SGB, wzrósł aż o **253%** w roku 2023, w stosunku do roku poprzedniego.

Produkty, które oferuje SALTUS Ubezpieczenia i które cieszą się największą popularnością wśród klientów to:

Acti Finanse Plus
ubezpieczenie na życie, które daje możliwość zabezpieczenia szerokiej gamy produktów kredytowych

SALTUS – Mój DOM NOWOŚĆ!
ubezpieczenie mieszkań i domów jednorodzinnych

SALTUS - Moje BEZPIECZEŃSTWO
ubezpieczenie Następstw Nieszczęśliwych Wypadków

SALTUS – Moja PODRÓŻ
ubezpieczenie podróżne

Włączenie do swojej oferty ubezpieczeń obu naszych towarzystw podniesie **konkurencyjność banku**, a także pozwoli lepiej odpowiedzieć na potrzeby klientów i zapewni **dodatkowe przychody pozaodsetkowe**.

SALTUS TUW – Towarzystwo majątkowe

oraz

SALTUS TU ŻYCIE SA – Towarzystwo życiowe

Zapraszamy do kontaktu i rozpoczęcia współpracy, która przyniesie korzyści zarówno Państwa instytucji, jak i Waszym klientom.

Piotr Gurgul
Dyrektor Zespołu Sprzedaży Ubezpieczeń – Banki Spółdzielcze

e-mail: piotr.gurgul@saltus.pl
tel. 609 562 832

Małgorzata Bacajewska
Z-ca Dyrektora Zespołu Sprzedaży Ubezpieczeń – Banki Spółdzielcze

e-mail: malgorzata.bacajewska@saltus.pl
tel. 603 950 341

TOWARZYSTWO UBEZPIECZONYCH

KLIKNIJ ŻEBY POSŁUCHAĆ ARTYKUŁU

OTWIERAMY PRZYSZŁOŚĆ DLA MŁODYCH

Ewelina Ignaczak
SGB-Bank SA

Przed nami Rok Edukacji Ekonomicznej. Czy narodowy program pogłębiania wiedzy Polaków o finansach i ekonomii jest nam potrzebny?

35% Polaków w wieku do 34 lat uważa, że jeśli w budżecie państwa brakuje pieniędzy, to należy je dodrukować, by uzupełnić lukę. To jedna z zaskakujących informacji, którą można znaleźć w raporcie z ogólnopolskiego panelu badawczego Ariadna. Co piąty Polak uznaje, że płacąc w sklepie, nie płaci podatku VAT. Przy okazji – tyle samo osób uważa, że hasło do bankowości elektronicznej warto zapisać w telefonie... Dla większości z nas przychód, dochód i zysk, to pojęcia tożsame i nie ma między nimi żadnej różnicy.

Te dane są bardzo niepokojące, choć niestety łatwo je sprowadzić do poziomu ciekawostki. Wskazują jak niski jest poziom wiedzy finansowej i edukacji ekonomicznej w naszym kraju. Pod tym względem jesteśmy na szóstym miejscu w Europie. Szóstym od końca.

Pozostając w sferze wniosków z badań, które dla mnie jako marketerki są niezwykle ważne, warto również zauważyć, że aż 40% dorosłych mieszkańców Polski opisuje swoją wiedzę finansową jako „wysoką". Dlaczego więc w obiektywnych badaniach naukowych w porównaniu do reszty Europy pozostajemy aż tak daleko w tyle? Jaka jest naprawdę nasza wiedza ekonomiczna? Czy warto zadbać, abyśmy o ekonomii wiedzieli więcej? A jeśli tak to dlaczego?

Edukacja ekonomiczna w „Tajemnicy Miasteczka"

Możemy mieć wpływ na poziom edukacji ekonomicznej. W Bankach Spółdzielczych SGB postawiliśmy na edukację młodego pokolenia, choć precyzyjniej byłoby napisać – dzieci. Jedną z naszych inicjatyw, w ramach nowej strategii komunikacji marki Banki Spółdzielcze SGB, jest gra internetowa „Tajemnica Miasteczka". W gronie najmłodszych popularyzuje ona ideę bankowości spółdzielczej, udostępnia podstawy wiedzy o finansach i jednocześnie promuje wartości ważne dla naszych banków oraz lokalnej społeczności – z wzajemnością.

Sięgnęliśmy po format gry komputerowej, ponieważ to najlepsze narzędzie dotarcia do bardzo młodych ludzi, przyszłych klientów banków spółdzielczych. Jesteśmy częścią lokalnych społeczności. Nasze relacje opierają się na wzajemnym wsparciu na każdym etapie życia, wspieraniu w rozwoju oraz wspólnym rozwiązywaniu problemów i podejmowaniu wyzwań. Ważna jest życzliwość i otwartość, także na zdobywanie nowej wiedzy. To buduje poczucie wspólnoty i podnosi jakość codziennego życia. O tym też jest nasza gra: o wzajemności i odpowiedzialności za własny rozwój i jego ekonomiczne podstawy.

OK, to tylko gra. Służy zabawie, zachęca do nauki. Świetnie działa i zbiera fajne recenzje, ale to „tylko" gra edukacyjna. Następny krok – własne konto i aplikacja dla młodych. W naszym przypadku nawet dla dzieci od 1. dnia życia! SGB Mobile w nowej odsłonie dla najmłodszych to wyższa szkoła jazdy – nauka

> Możemy mieć wpływ na poziom edukacji ekonomicznej. W Bankach Spółdzielczych SGB postawiliśmy na edukację młodego pokolenia, choć precyzyjniej byłoby napisać – dzieci.

bankowania na żywo i całkiem na serio. Możesz kontrolować swoje wydatki nawet w wieku kilku lat! Możesz mieć źródło szybkiej analizy – na co wydajesz kieszonkowe, gdzie uciekają pieniądze, jakie wydatki można ograniczyć, by zaoszczędzić na przyjemności?
Dzieci wybierają w SGB Mobile własnego awatara. Karta do konta ma design stworzony na podstawie rekomendacji grupy docelowej. Ich konto uwzględnia wszystkie potrzeby młodego klienta, w tym zakupy internetowe, a jego rodzicom daje komfort dyskretnej, bezpiecznej kontroli nad wydatkami latorośli.

Jak wykorzystać potencjał banków spółdzielczych

A zatem – edukacja już kilku-kilkunastolatków, połączona z aktywnym korzystaniem z narzędzi finansowych. To system naczyń połączonych. Nauka i praktyka w jednym, jako najlepszy sposób pogłębiania świadomości ekonomicznej. Nie ma lepszej drogi.
Im więcej wiemy na temat finansów, tym szybciej bogacimy się i łatwiej znajdujemy narzędzia, które pozwalają nam zwiększyć zarobki lub założyć dobrze prosperujący biznes. Stan umiejętności społecznych w kategoriach tak oczywistych jak inwestowanie, oszczędzanie czy znajomość praw i obowiązków wiążących się z zaciągniętymi zobowiązaniami, może mieć bezpośredni wpływ na potencjał rozwojowy całego państwa. Silną gospodarkę zbudować mogą tylko świadomi ekonomicznie obywatele.
Kto jest za to odpowiedzialny? Rodzice? Szkoła? Wyższe uczelnie? Telewizja? A może przedsiębiorstwa, banki? Wspólną odpowiedzią może być Rok Edukacji Ekonomicznej – narodowy program, którego zadaniem jest pogłębianie wiedzy o ekonomii jako podstawie do rozwijania majętności Polaków. Mieszczą się w nim zadania dla wszystkich wymienionych powyżej podmiotów, w tym banków. Także – banków spółdzielczych.

Z perspektywy banków spółdzielczych te działania mają jeszcze jeden walor – lokują je w świadomości młodych. Pozwalają zbierać wokół idei bankowości spółdzielczej nową społeczność. To dla niej można przygotowywać różne inicjatywy – webinary, warsztaty, prezentacje, spotkania dotyczące podstawowych zagadnień ekonomicznych, takich jak zarządzanie finansami osobistymi, oszczędzanie i inwestowanie. To jest grupa potencjalnych odbiorców materiałów edukacyjnych, służących zrozumieniu podstawowych pojęć ekonomicznych.

A zatem – edukacja już kilku – kilkunastolatków, połączona z aktywnym korzystaniem z narzędzi finansowych. To system naczyń połączonych. Nauka i praktyka w jednym, jako najlepszy sposób pogłębiania świadomości ekonomicznej. Nie ma lepszej drogi.

Banki spółdzielcze mają doskonały potencjał, by współpracować ze szkołami i organizacjami młodzieżowymi. Cel? Edukacja, rozwój osobisty, tworzenie nawyków bezpiecznego korzystania z narzędzi finansowych dla najmłodszych klientów. Uczenie ich, że dbanie o siebie to również dbanie o swoje pieniądze. W podobny sposób można współpracować z uczelniami – a przypomnę, że ideą naszej oferty dla młodych jest prowadzenie ich kont do pełnoletniości i ich płynna „zamiana" na konta dorosłych klientów. Można te działania wzmocnić poprzez tematyczne wykłady na uczelniach, staże w bankach, warsztaty i spotkania dotyczące ekonomii i finansów, a przy okazji edukacji na temat wartości stojących u podstaw działania bankowości spółdzielczej.
Tak właśnie wyobrażam sobie dbanie o naszych klientów – na każdym etapie ich życia. To dbanie może też mieć wyraz w realizacji przedsięwzięć edukacyjnych, wspierających rozwój osobisty i wiedzę.

Przyszłość w... dbałości, uważności i konsekwencji.

Jesteśmy ważnym elementem lokalnych społeczności. To jest zobowiązanie i jednocześnie duża korzyść – znamy wielu naszych klientów bezpośrednio, są naszymi sąsiadami z podwórka, ulicy, szkoły, dzielnicy czy firmy. Jest nam dużo łatwiej określić nie tylko potrzeby lokalnych konsumentów, ale i stan świadomości, która służy ich generowaniu.
Ale potrzeby nie ujawnią się same, trzeba je badać, oceniać, wspierać klientów w pozyskiwaniu wiedzy i wyposażać ich w odpowiednie narzędzia. Czasem będzie to gra komputerowa, czasami komunikacja w social mediach, a w innych przypadkach – pogłębiona dyskusja o instrumentach finansowych i gotowe narzędzia do bankowania.
W każdym przypadku historia zaczyna się od wiedzy. Odpowiedni sposób jej przekazania, prezentowania w działaniach, konsekwencji w ich realizacji daje większe szanse na rozwój nie tylko ekonomiczny, ale przede wszystkim społeczny. To na tym nam zależy, to jest podstawą naszej bankowej misji – nie tylko w Roku Edukacji Ekonomicznej, ale w kolejnych latach, w całej naszej przyszłości. ●

Artykuł został również opublikowany w Głosie Banków Spółdzielczych nr 1/2024

WIEDZA FINANSOWA W CENIE

Janusz Orłowski

Decyzją Senatu RP obecny rok został ustanowiony Rokiem Edukacji Ekonomicznej i stanowi formę docenienia wysiłków wielu tysięcy osób i instytucji zaangażowanych na przestrzeni ostatnich stu lat w popularyzację i przekazywanie tej ważnej wiedzy oraz wsparciem dla działań podejmowanych obecnie przez instytucje publiczne i pozarządowe organizacje społeczne. Stanowi także okazję do przypomnienia reform i inicjatyw gospodarczych Władysława Grabskiego oraz idei edukacji ekonomicznej.

Badania Fundacji Kronenberga

O tym, że taka edukacja jest wciąż potrzebna świadczą m.in. badania Fundacji Kronenberga, działającej przy banku Citi Handlowy, która od wielu lat bada finansowe postawy i zachowania Polaków. Z ostatniego takiego badania wynika, że zmniejszył się odsetek naszych rodaków, którzy planują krótkoterminowo swoje wydatki, zwiększył natomiast odsetek tych, którzy w ogóle nie planują wydatków. Taka postawa z pewnością potwierdza konieczność podejmowania działań zmierzających do lepszej edukacji finansowej naszych rodaków. Inicjatywa podjęta przez Senat RP trafiła więc na podatny grunt i powinna przyczynić się do uświadomienia Polakom, jak ważną kwestią jest wiedza ekonomiczna.

Spadek odsetka osób deklarujących kontrolę nad swoimi wydatkami może się wydawać zaskakujący w obliczu wzrastającej niepewności związanej z epidemią oraz jej gospodarczymi konsekwencjami, jak również sytuacją u naszego wschodniego sąsiada. Sprawdzanie wydatków obejmuje przede wszystkim regularne kontrolowanie zasobów finansowych, które mamy do swojej dyspozycji. Tylko nieco ponad połowa Polków deklaruje, że regularnie sprawdza stan konta bankowego lub zawartość portfela oraz poczynionych wydatków.

Bardzo niewiele osób prowadzi w systematyczny sposób swój budżet – czy to w Excelu lub wersji papierowej, czy w specjalnych programach i aplikacjach. Najczęściej robią to seniorzy, co jednak może wynikać z tego, że posiadają ograniczone środki i prowadzenie budżetu pozwala im lepiej nimi zarządzać.

Badania pokazały, że dwie trzecie naszych rodaków deklaruje przekonanie do oszczędzania. Rośnie ono wraz z wiekiem. Odsetek Polaków, którzy odkładają część pieniędzy od lat pozostaje na zbliżonym poziomie sześćdziesięciu kilku procent. Jednak w większości przypadków oszczędzanie ma charakter sporadyczny, a nie regularny. Zdecydowanie najrzadziej oszczędzają najmłodsi, ale istotnym czynnikiem jest także wykształcenie. Oszczędzanie deklaruje 80% osób z wykształceniem wyższym, a tylko 48% z wykształceniem podstawowym.

Nie oszczędzają, bo mało zarabiają

Nasi rodacy deklarują, że nie odkładają pieniędzy przede wszystkim z powodu zbyt małych zarobków. Przyczynę taką wskazało więcej niż połowa respondentów. Jedna piąta Polaków w wieku od 25 do 39 lat zadeklarowała, że nie ma nawyku odkładania pieniędzy, co może wynikać m.in. z doświadczeń wcześniejszego okresu życia, kiedy nie dysponowali własnymi pieniędzmi i nie ukształtowali w sobie praktyk związanych z oszczędzaniem. Zdaniem autorów badania grupa ta może być interesującym adresatem działań edukacyjnych – ma już bowiem własne dochody oraz pewną świadomość ograniczonej własnej kompetencji w kwestii zarządzania finansami.

Dla osób najstarszych, powyżej 60. roku życia, znaczącą przeszkodą w oszczędzaniu są bieżące wydatki. Jednocześnie seniorzy często deklarują, że mają już wszystko, czego potrzebują, nie mają więc jasnego celu, który motywowałby ich do oszczędzania. Nie są też pewni swojej przyszłości i nie wiedzą czy warto budować finansowe zabezpieczenie.

Wzrósł natomiast odsetek Polaków, którzy odkładają nie tylko na konkretne cele, ale ze względu na chęć zabezpieczenia przyszłości, na tzw. czarną godzinę lub na wypadek pojawienia się nagłych, nieprzewidzianych okoliczności. Tendencja ta wzrasta wraz z wiekiem. Obawy wobec przyszłości zwiększają prawdopodobnie motywacje do budowania „poduszki finansowej", która daje poczucie bezpieczeństwa w niepewnych czasach.

Oszczędności Polaków nie stanowią jednak wielkiego kapitału – prawie połowa deklaruje, że nie przekraczają one wysokości trzymiesięcznych dochodów. Tylko jedna czwarta naszych rodaków, która zadeklarowała, że oszczędza, byłaby w stanie żyć z posiadanych środków powyżej trzech miesięcy, bez obniżania poziomu dotychczasowego życia.

Oszczędzanie z myślą o emeryturze

jest wciąż bardzo mało rozpowszechnione wśród Polaków. Od lat odsetek takich osób oscyluje wokół 10%. Skłonność do oszczędzania na ten cel rośnie jednak wraz z wiekiem. Zdecydowanie częściej niż inni oszczędzają na emeryturę przedsiębiorcy oraz osoby z wyższym wykształceniem.

Ponad jedna czwarta Polaków posiadających dzieci deklaruje, że oszczędza na nie pieniądze. Trzeba jednak podkreślić, że co trzeci respondent nie był w stanie oszacować jaką kwotę odkłada miesięcznie na dziecko, co pokazuje, że praktyka ta nie jest bardzo systematyczna i przemyślana. Program 500 plus jest dla Polaków głównym źródłem środków odkładanych z myślą o dzieciach. Połowa pytanych o tę kwestię zadeklarowała, że czerpie odkładane pieniądze właśnie z tego wsparcia. Polacy, którzy gromadzą oszczędności dla dzieci lokują je najczęściej na koncie bankowym i nie starają się ich pomnożyć poprzez inwestowanie.

Niemal połowa badanych Polaków uważa, że w kwestiach dotyczących oszczędzania i inwestowania, ufa przede wszystkim sobie – własnej wiedzy, doświadczeniu i intuicji. Zdecydowanie rzadziej wyrażają podobne zaufanie wobec znajomych czy instytucji finansowych lub mediów. Taka postawa, to również uzasadnienie dla potrzeby prowadzenia edukacji ekonomicznej, która powinna być dostępna już dla naszych najmłodszych rodaków, czyli uczniów szkół podstawowych. ●

O EDUKACJI FINANSOWEJ MÓWIĄ

W tym roku przypada 100-lecie reform gospodarczych Władysława Grabskiego, powstania polskiego złotego i Banku Polskiego oraz Banku Gospodarstwa Krajowego, a także wydania książki Janusza Korczaka „Bankructwo Małego Dżeka". Aby to uczcić Senat, na czele którego mam zaszczyt stać, ustanowił rok 2024 Rokiem Edukacji Ekonomicznej. Chcemy w ten sposób przypomnieć znaczenie tych wydarzeń w historii odradzającego się państwa polskiego oraz podkreślić znaczenie edukacji ekonomicznej we współczesnym świecie.
„Kierując się słowami Władysława Grabskiego: «Edukacja ekonomiczna stanowi fundament dobrobytu narodowego i osobistego», chcemy wzmocnić dążenia świata ekonomii i edukacji do podmiotowej obecności edukacji ekonomicznej w polskim życiu społecznym, gospodarczym i politycznym" – napisali senatorowie w uchwale z 7 września 2023 r.
Jako członek Honorowego Komitetu Obchodów Roku Edukacji Ekonomicznej pragnę zapewnić, że Senat będzie wspierać inicjatywy i działania popularyzujące wiedzę ekonomiczną i finansową. We współczesnym, szybko zmieniającym się świecie edukacja w tym zakresie jest niezbędna nie tylko dla dzieci i młodzieży, ale także dla dorosłych.
Komitet jest dobrą platformą do rozwijania współpracy z odpowiednimi Ministerstwami – Edukacji i Finansów – w obszarze podnoszenia u młodych ludzi zainteresowania edukacją ekonomiczną. Dzieci i młodzież powinny wiedzieć, jak dobrze zarządzać własnym budżetem, bo wtedy będą mogły łatwiej zrozumieć, jak tworzony i zarządzany jest budżet naszego Państwa. Oczekuję, że będziemy nad tym bardzo aktywnie pracować, by od najmłodszych lat edukacja ekonomiczna była stałym elementem rozwijania umiejętności polskich uczniów. Chcemy bowiem przygotować młode pokolenie do udziału w budowie nowoczesnej gospodarki, odpowiadającej na wyzwania naszych czasów.

Marszałek Senatu RP – Małgorzata Kidawa-Błońska

Zainaugurowane przez Senat RP obchody Roku Edukacji Ekonomicznej 2024 to bardzo dobry pomysł. Zainicjowanie w roku bieżącym dyskusji na poziomie ogólnokrajowym na temat potrzeby edukacji ekonomicznej uwzględniającej współczesne wyzwania to niezwykle potrzebna inicjatywa. Należy ją wykorzystać dla rozwoju myśli ekonomiczno-finansowej społeczeństwa polskiego. Pamiętam, jak swego czasu w bankowości spółdzielczej pracowaliśmy, aby zapobiec ekonomicznemu wykluczeniu wiejskich środowisk po likwidacji w Polsce m.in. PGR-ów.
Środowiska byłych pracowników likwidowanych państwowych gospodarstw rolnych nie miały zapewnionej obsługi finansowej, nie miały wiedzy na temat zasad korzystania z bankowości. Robiliśmy dla tych środowisk akcje uświadamiające, zachęcające je do korzystania z nowych instrumentów finansowych, z nowych usług, produktów. Staraliśmy się przeciwdziałać wykluczeniu ekonomiczno-finansowemu.
Dzisiaj sytuacja ekonomiczna Polaków jest już zupełnie inna, ale nadal jest wiele rzeczy do zrobienia w zakresie szerzenia wiedzy finansowej. Mam na myśli na przykład umiejętność korzystania z nowych usług banków oferowanych w bankowości internetowej i mobilnej, jakie zapewniają banki spółdzielcze.
Tempo rozwoju technologicznego jest na tyle szybkie, że wymaga od nas wszystkich złożonej wiedzy ekonomicznej i technologicznej.
Dzisiejsze, dobrze prowadzone przedsiębiorstwo musi się opierać na zdrowych zasadach ekonomicznych. Trzeba kształcić młodzież, bo to ona za chwilę będzie tworzyła firmy, organizowała przedsiębiorstwa, wyłonią się spośród niej nowi, młodzi menadżerowie, którzy poprowadzą swoje firmy i konieczna im będzie rzetelna wiedza ekonomiczna. Dlatego uważam, że trwający obecnie Rok Edukacji Ekonomicznej 2024 jest niezmiernie ważny i potrzebny.

Jan Grzesiek, przewodniczący Rady Nadzorczej SGB-Banku SA

Finansowa edukacja w naszym polskim mindsecie uwikłana jest w pewien paradoks. Jej wysoka rola w osiąganiu dobrobytu gospodarstw domowych wydaje się odwrotnie proporcjonalna do pozbawionej emocji reakcji przeciętnego obywatela na hasło „finanse osobiste". Czy Rok Edukacji Ekonomicznej może to zmienić? Pod pewnymi warunkami. Najważniejsze, by nie pozostał w gronie zafascynowanych nim organizatorów. Jak wejść pod strzechy? Na pewno nie wprost. Życzę nam wszystkim odważnej kampanii, która nie bierze jeńców, a do rozmów o pieniądzach skłania w przysłowiowej kolejce do lekarza. Lubimy się tam otworzyć przed obcym, żeby oswoić strach. O finansach też często łatwiej mówić groźbą niż prośbą. I chyba wciąż nie doceniamy na tym polu języka korzyści, na którym rosną fin-edukatorzy nowego pokolenia. Pokaż mi, jakie mam opcje i naucz swobodnie sięgać po produkty finansowe. Ale nie tylko depozytowe i nie tylko, gdy stopy biją rekordy. Powiedz, jak mogą mi się przydać produkty bankowe, nie mówiąc jakie masz dla mnie produkty bankowe. Trudne? W sam raz do rozgryzienia na ten rok.

Malwina Wrotniak, dziennikarka ekonomiczna, autorka finansowego bloga DrodzyRodzice.pl

Ubezpieczenie domu i mieszkania w Generali

– dlaczego warto?

Jedną z głównych przewag, która wyróżnia ofertę Generali spośród konkurencji, jest zwiększenie zakresu odpowiedzialności wynikającej z „zapominalstwa”. Pomimo braku wykonania przeglądów budowlanych (gazowego, kominiarskiego), czy braku wyczyszczenia przewodów kominowych, Generali będzie teraz odpowiadać za szkodę do pełnej sumy ubezpieczenia budynku, niezależnie od jego wieku. W przypadku braku przeglądu elektrycznego odpowiedzialność warunkowana jest wiekiem budynku – max 35 lat. Ta odważna decyzja podkreśla zaufanie firmy do swoich klientów i gotowość do wychodzenia naprzeciw ich potrzebom

Konrad Słonecki
Menedżer ds. Rozwoju
Ubezpieczeń Majątku
Indywidualnego, Generali Polska

Ponadto, Generali wprowadziło dodatkową ochronę przed zalaniem lub kradzieżą. Jeżeli klient zapomni zamknąć okno, drzwi lub balkon, a w konsekwencji dojdzie do zalania lub kradzieży, Generali wypłaci świadczenie do kwoty 20 000 zł.

Kolejny wyróżnik to rozszerzenie ochrony w przypadku kradzieży samochodu osobowego. Dotychczas ubezpieczenie obejmowało jedynie pojazdy zaparkowane w garażu wolnostojącym. Teraz Generali rozszerza to na samochody zaparkowane w podziemnych garażach budynków wielorodzinnych, na miejscach przypisanych do lokali mieszkalnych. Co więcej, limit ochrony został podniesiony aż do 35 000 zł.

Wychodząc naprzeciw zmieniającym się potrzebom klientów, Generali wprowadziło również możliwość ubezpieczenia robotów koszących od kradzieży z terenu posesji. To rozwiązanie szczególnie docenione przez klientów, którzy coraz częściej korzystają z nowoczesnych technologii, dbając jednocześnie o ich ochronę.

W ofercie Generali znalazła się także opcja ubezpieczenia lokalu segmentu wraz z dachem i płotem do niego przylegającym, niezależnie od udziału w częściach wspólnych. Generali ubezpieczy ten typ lokalu w wartości rynkowej, co daje klientom pełne poczucie bezpieczeństwa i zabezpieczenia swojej inwestycji.

Jeszcze jedną interesującą przewagą jest przyjęcie odpowiedzialności za szkody wyrządzone przez dzieci poniżej 13. roku życia, gdy nie można przypisać winy w nadzorze przedstawiciela ustawowego (bez szkód wyrządzonych w elektronice) . – Ta elastyczność i wyrozumiałość jest wyrazem zaufania, jakim obdarzamy naszych klientów. Chcemy, żeby mieli poczucie, że mogą na nas naprawdę liczyć w trudnych chwilach.

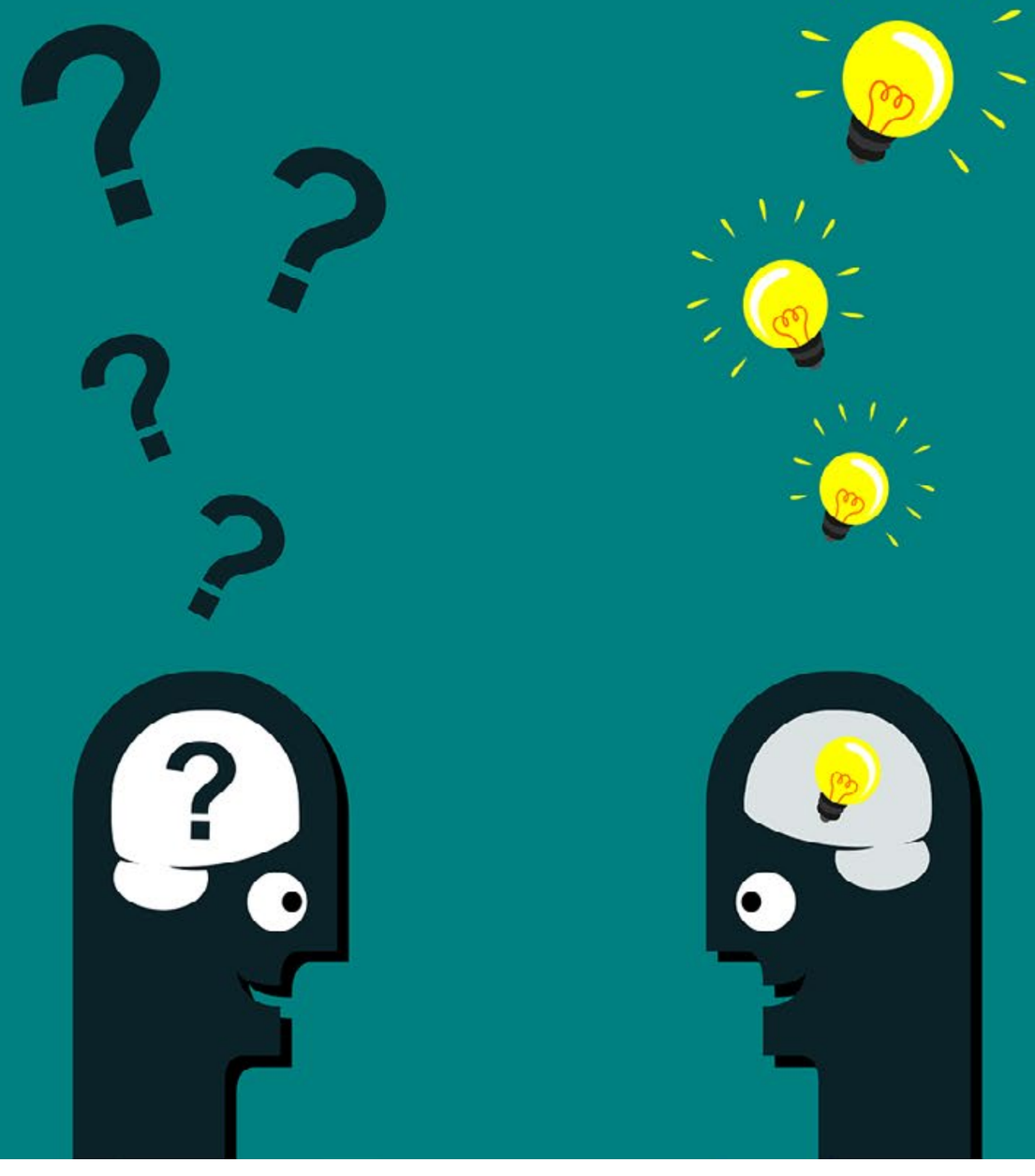
W przypadku wystąpienia katastrofy budowlanej, pożaru, silnego wiatru, wybuchu, powodzi, zalania w wyniku akcji ratowniczej, które uniemożliwiają zamieszkanie w ubezpieczonym lokalu, Generali pokrywa koszty wynajęcia lokalu zastępczego. Limit tej opcji wynosi 25 000 zł (bez ograniczenia czasowego) co pozwala na zapewnienie odpowiedniego miejsca zamieszkania w trudnych okolicznościach.

Generali oferuje także pakiet medyczny, który zawiera telekonsultacje, badania oraz rehabilitację po nieszczęśliwym wypadku. Warunkiem skorzystania z takiej pomocy medycznej jest zalecenie przez lekarza – unieruchomienia kończyny lub kręgów szyjnych na okres co najmniej 7 dni. Dzięki temu pakietowi, ubezpieczony ma dostęp do specjalistycznej opieki medycznej w razie wypadku. Limit na ten pakiet wynosi 3 000 zł, co daje możliwość skorzystania z dodatkowej pomocy medycznej w potrzebie.

W przypadku kradzieży z włamaniem, Generali zapewnia ochronę rzeczy ubezpieczonego znajdujących się w metalowych boksach lokatorskich oraz w piwnicach, które posiadają drzwi z drewnianych sztachet. Dzięki temu ubezpieczony ma pewność, że jego mienie jest dodatkowo zabezpieczone przed potencjalnymi stratami w przypadku włamania.

Generali oferuje także możliwość zabezpieczenia się przed kradzieżą z włamaniem do domu, który jest jeszcze w budowie. Ta opcja pozwala na zabezpieczenie mienia podczas trwania prac budowlanych, dając ubezpieczonemu spokój i ochronę w trakcie procesu budowy domu.

CZY PROSTY JĘZYK JEST KONIECZNOSCIĄ?



W SGB-Banku SA prowadzimy program „Się rozumie”, w którym edukujemy banki i naszych pracowników, jak skutecznie korzystać z prostego języka. Sami jednak mamy wątpliwości i pytania, a odpowiedzi na nie najlepiej zostawić specjalistom. W tym roku w naszym magazynie będziemy co kwartał zadawać pytania znakomitym polskim językoznawcom. Teraz – prof. UAM dr hab. Jarosław Liberek.

Rafał Łopka
SGB-Bank SA

1. Prosty język w bankowości – moda czy konieczność?

Wprowadzanie prostego języka do bankowości stało się trochę modne. Powstał rynek usług prostojęzycznych, szkoleniami z upraszczania zajmuje się dużo osób, choć nie zawsze mają one odpowiednie kompetencje.

Czy prosty język jest koniecznością? W sensie formalnym – nie, bo nie ma przepisów wymuszających proste pisanie. Tworzenie klarownych pism oficjalnych jest natomiast koniecznością w sensie społecznym i instytucjonalnym. Komunikacja publiczna stała się niezwykle zapętlona w swej niezrozumiałości. Trzeba do niej wprowadzać jak najwięcej prostoty, bo tylko to, co proste, ma szanse być wspólne. Wszelkie komplikacje tekstowe mogą powodować, że ktoś czegoś nie zrozumie, czyli znajdzie się poza wspólnotą.

2. Czy nadmierna poprawność językowa i dążenie do precyzyjności za wszelka cenę może zaciemnić przekaz?

Skrajna normatywność może utrudnić odbiór przekazu np. wtedy, gdy piszący skupi się na poprawności i nie zauważy, że w jego tekście przyczyną ewentualnych niepo-

> Do Poradni Językowej UAM dzwonią osoby, które w jednym ręku trzymują słuchawkę, w drugim pogmatwane pismo z jakiejś instytucji, cytują je i proszą o przetłumaczenie z polskiego na nasze.

rozumień nie będzie wyraz budzący zastrzeżenia normatywne, ale zbyt skomplikowana konstrukcja składniowa. Wyobraźmy sobie, że urzędnik redaguje przepisy porządkowe dotyczące manualnej relokacji psich ekskrementów do dedykowanych pojemni-

ków śmieciowych. W uproszczeniu takiego zdania nie pomoże zastanawianie się nad zasadnością użycia słowa dedykowany. Ten imiesłów raczej nie będzie budził, szczególnie w młodszych pokoleniach, zdziwienia. Czytelnik przepisów miejskich zacznie się jednak zastanawiać, o co chodzi w tej manualnej relokacji i co to takiego psie ekskrementy. Byłoby o wiele lepiej, gdyby urzędnik napisał o wyrzucaniu psich kup do koszy. Pomijam już, że w tym zdaniu irytująca jest również nadgorliwość piszącego, który mówi obywatelowi, co ma zrobić z psią kupą. Tymczasem istotą rzeczy jest obowiązek posprzątania, a sposób posprzątania to sprawa drugorzędna. Obywatel może kupę wyrzucić do kosza, ale jeśli przyjdzie mu ochota, może też zanieść do domu i spuścić w sedesie…

> Wprowadzanie prostego języka do bankowości stało się trochę modne. Powstał rynek usług prostojęzycznych, szkoleniami z upraszczania zajmuje się dużo osób, choć nie zawsze mają one odpowiednie kompetencje.

3. Co sądzi Pan o braku poprawności w dzisiejszym języku, zwłaszcza w mediach społecznościowych, SMS-ach czy mejlach?

Nawet pobieżna lektura przekaźników elektronicznych pokazuje, że dziwacznych odstępstw od normy mamy dużo. Z mojego prywatnego archiwum mogę podać chociażby takie przykłady różnych zakłóceń: Nasza partia jest za in witrem; Zwierzęta boją się w sylwestra fajerwerk; Bezdomny, żebrując pod sklepem, wymuszał pieniądze; Z powodu huraganu Norwedzy siedzą w domach; Samochody importujemy z Włoszech; Przestępca nie pałał się żadnym zajęciem; Piłkarz gra od deski do deski (w znaczeniu „cały mecz”); Szef stosuje w zarządzaniu metodę bata i marchewki; Politycy podczas kampanii sądzą gruszki na wierzbie; Wypowiedź trenera była jak spleśniała wisienka na śmierdzącym torcie; Budowa ośrodka ślimaczy się niemrawo. Takie błędy świadczą o spadającej kompetencji komunikacyjnej Polaków. Nie da się tego zatrzymać. Jedyne pocieszenie jest takie, że bardzo często naruszenia normy nie powodują braku porozumienia. Odbiorcy dzięki intuicji zazwyczaj domyślają się, co poeta miał na myśli.

4. Jak często w Poradni Językowej, którą prowadzi pan od wielu lat, pytania dotyczą prostego języka i jasnego przekazu?

Do Poradni Językowej UAM dzwonią osoby, które w jednym ręku trzymują słuchawkę, w drugim pogmatwane pismo z jakiejś instytucji, cytują je i proszą o przetłumaczenie z polskiego na nasze. Takich pytających jest coraz więcej. Ostatnio stworzyliśmy nawet na UAM specjalną Poradnię Prostego Języka. Gdybym dokładnie policzył, to mimo wszystko pytania z zakresu stylistyki i frazeologii, gramatyki, semantyki oraz ortografii i interpunkcji dominują.

5. Na co pana zdaniem w pierwszej kolejności powinni zwrócić uwagę bankowcy w pismach do klientów?

Komplikacja formalna, a więc wieloelementowe konstrukcje składniowe i zdania liczące po kilkadziesiąt słów, to najpoważniejszy mankament. Widoczny jest szczególnie w umowach oferowanych klientom. Oprócz tego redaktorzy bankowi muszę zwracać uwagę na zależność tworzonych pism od przepisów. Kopiowanie obszernych fragmentów różnych ustaw i regulaminów nie służy porozumieniu. Niestety, nawet jeśli twórcy tekstów potrafią je napisać prosto, często na przeszkodzie stają prawnicy. Jak przekonać tych strażników skostniałego stylu? To bardzo duży problem, gdyż ci strażnicy nie chcą podcinać gałęzi, na której siedzą. ●

Prof. UAM dr hab. Jarosław Liberek, wybitny językoznawca, wykładowca na Wydziale Filologii Polskiej i Klasycznej UAM, kierownik studiów podyplomowych „Prosty język w instytucjach publicznych”, a ponadto Telefonicznej Poradni Językowej i Pracowni Leksykograficznej; współautor czterech słowników frazeologicznych, autor wielu innych prac naukowych.

NASI KLIENCI SĄ JAK KORZENIE
SPÓŁDZIELCZE
SŁOWO ROKU 2023

Joanna Gębka
SGB-Bank SA

Katarzyna Miler
SGB-Bank SA

Jędrzej Szymanowski
SGB-Bank SA

Pod koniec zeszłego roku po raz drugi przeprowadziliśmy plebiscyt Spółdzielcze Słowo Roku. Naszą inspiracją było Młodzieżowe Słowo Roku, czyli ranking, który od lat organizuje PWN we współpracy z Uniwersytetem Warszawskim. MSR odzwierciedla trendy, jakie rodzą się w języku najmłodszych pokoleń Polaków i na kilka tygodni staje się pożywką copywriterów prześcigających się w coraz to bardziej „zabawnych" reakcjach na propozycje młodzieży. W tym roku zwyciężyło słowo rel. To wyrażenie od ang. relatable, czyli możliwy do powiązania z tematem. Stosuje się je jako potwierdzenie tego, co mówił przedmówca, a nawet utożsamienie się z jego wypowiedzią.

Spółdzielczy slang

A w jaki sposób ze spółdzielczością utożsamiają się pracownicy Grupy SGB? Ponownie postanowiliśmy to sprawdzić i przystąpiliśmy do zbierania propozycji na Spółdzielcze Słowo Roku. Szczególnie, że ubiegłoroczna akcja cieszyła się sporym powodzeniem. Przyjmowaliśmy słowa lub wyrażenia, które:

- są popularne w naszym zrzeszeniu,
- są proste i zrozumiałe dla wszystkich – zgodnie ze standardami „Się rozumie",
- nie są wulgarne i obraźliwe.

Jeszcze jedno: w plebiscycie nie brał udziału zwycięzca z poprzedniego roku, czyli słowo przyszłość.

SPÓŁDZIELCZE SŁOWO ROKU

Po raz kolejny otrzymaliśmy dużą liczbę zgłoszeń, które następnie poddaliśmy pod głosowanie pracownikom Banków Spółdzielczych SGB i SGB-Banku SA. Jaki obraz spółdzielczości widzimy, kiedy weźmiemy pod językową lupkę te propozycje? Z całą pewnością – pozytywny! Podobnie jak w ubiegłym roku, pracownicy postawili na zrzeszeniowe wartości. *Współpraca, wspólnie, razem* i przekonanie, że *dobrze dbać o siebie nawzajem* – to nie tylko hasła naszej marki, to nasza codzienność. To, że znów pojawiły się w plebiscycie podkreśla tylko *jedność i nierozerwalność* SGB. Po prostu tacy jesteśmy i to jest dla nas ważne.

Pamiętamy jednak, że tej dobrej współpracy nie ma bez *zaufania, odpowiedzialności* czy *regularnego feedbacku* między nami. Naturalnym jest więc, że spółdzielcy zadbali, aby i te wyrażenia pojawiły się wśród kandydatów na Spółdzielcze Słowo Roku.

> Z tegorocznego plebiscytu mocno wybija się fakt, że wszystko, co robimy, to działania dla… klientów. Dobrze uzasadnia to reprezentacja takich wyrażeń jak *gość*, *korzenie* czy *swojski*, wraz z ich znaczeniami *(ludzie dla ludzi)*.

Co jeszcze widzimy, kiedy przyglądamy się tej ciekawej liście? To, co najbardziej angażowało nas przez 12 miesięcy ubiegłego roku. Jednym z tematów, który dominował w jego drugiej połowie jest kredyt płynnościowy dla rolników. W naszym plebiscycie ma on reprezentację w postaci aż dwóch wyrażeń – *płynnościówka* i *UP*. 2023 to też rok, kiedy zrobiliśmy naprawdę duży krok w stronę młodości. Dla młodych klientów przygotowaliśmy karty przedpłacone, grę „Tajemnica Miasteczka" czy ofertę SGB Junior.

Banki Spółdzielcze SGB to od dawna zielone banki – w dosłownym i przenośnym znaczeniu. Banki, które oferują ekologiczne rozwiązania, np. kredyt *czyste powietrze*, i dbają o swoje zielone sąsiedztwa. O EKO w tym roku też trudno było nie mówić, skoro na horyzoncie pojawiło się ESG.

Z tegorocznego plebiscytu mocno wybija się fakt, że wszystko, co robimy, to działania dla… klientów. Dobrze uzasadnia to reprezentacja takich wyrażeń jak *gość*, *korzenie* czy *swojski*, wraz z ich znaczeniami *(ludzie dla ludzi)*.

A jeśli o ludziach mowa, to podkreślana i wyróżniana była też praca Menadżerów Zrzeszeniowych – do listy zakwalifikował się skrót MZ. Brawo dla nich!

W kontekście tego, co dzieje się na świecie, trudno też nie zwrócić uwagi na priorytetową kwestię *bezpieczeństwa*.

Nasz wewnętrzny plebiscyt, podobnie jak ten PWN, traktujemy z dystansem. Nie jest on lustrem, ale trochę pokazuje jacy jesteśmy i co jest dla nas ważne. Wybija się z niego to, co najbardziej zajmowało nas w tym roku – z czym się mierzyliśmy i co było dla nas wyzwaniem. Cieszy nas, że większość tych propozycji to reprezentacja naprawdę pięknych wartości. Mało na tej liście neologizmów czy zapożyczeń. Nie oznacza to jednak, że innowacji nie ma. Zgłaszający opierali się głównie na znanych słowach, ale nadali im nowy – ciekawy, spółdzielczy kontekst. Wyszły naprawdę sympatyczne *kocury* (to również słowo zgłoszone do rankingu)!

Stabilne drzewo spółdzielczości

A co po głosowaniu? Spółdzielczym Słowem Roku 2023 zostało słowo korzenie, jako określenie klientów:

Nasi klienci są jak korzenie, stabilne drzewo spółdzielczości.

To tylko potwierdza, że nasze priorytety pozostały niezmienne. Wszystko, co robimy, robimy przecież dla klientów. To oni ostatecznie są najważniejszymi konsumentami produktów i usług, które im oferujemy.

Klienci jako korzenie – pięknie wpisuje się to w hasło naszej marki. Przez ostatnie dwa lata głośno komunikowaliśmy przecież, że w SGB dobrze dbać o siebie nawzajem. Naszą siłą, a przede wszystkim tym, co odróżnia nas od innych banków, jest to, jak dbamy o relacje. I robimy to nie od wczoraj, nie od dwóch lat, ale od dawna. Bo w DNA banków spółdzielczych wpisana jest lokalność, wzajemność i społeczność. I może właśnie dzięki temu możemy z dumą i wdzięcznością pisać o klientach w kontekście korzeni, a nie ziarenek, które dopiero muszą wykiełkować. Te korzenie to po prostu wiele lat tradycji każdego lokalnego Banku Spółdzielczego SGB. Korzenie to fundament. Choć często ich nie widać, są najważniejsze i to właśnie o nie trzeba najbardziej dbać. Od korzeni po prostu wszystko się zaczyna i często na korzeniach kończy.

Nie możemy nie wspomnieć też o ekologicznym kontekście korzeni. Banki Spółdzielcze SGB to w końcu też banki, które dbają o całe otoczenie. Tworzą i rozwijają zielone sąsiedztwa. W tej wizji wręcz naturalnym jest skojarzenie klientów z korzeniami. Zupełnie jak w naszej reklamie z kampanii Taka różnica!

> *Kocur* to dla nas definicja nieszablonowego i kreatywnego myślenia, do którego żarliwie zachęcamy Was w tym plebiscycie.

Kocur z wyróżnieniem kapituły

Jako jury Spółdzielczego Słowa Roku 2023 postanowiliśmy przyznać też jedno wyróżnienie. Wyróżniliśmy **kocura**, który do plebiscytu został zgłoszony w znaczeniu:

Coś fajnego, świetna idea, dobry pomysł, coś nietuzinkowego.

Subiektywnie doceniliśmy – nomen omen – nieoczywistość i pomysłowość tej kandydatury. Kocur to dla nas definicja nieszablonowego i kreatywnego myślenia, do którego żarliwie zachęcamy Was w tym plebiscycie. Kto wie, może *kocur* na stałe *zakorzeni się* w naszym wewnętrznym spółdzielczym języku? ●

CHRISTINE LAGARDE – TWARDA KOBIETA NA WYSOKICH OBCASACH

Jej syn stracił majątek na inwestycjach w kryptowaluty. „Zignorował mnie" – powiedziała podczas spotkania ze studentami we Frankfurcie, wyjaśniając, że jest zdecydowaną przeciwniczką wirtualnej waluty. Akurat z jej zdaniem syn powinien się liczyć: Christine Lagarde jest przecież prezeską Europejskiego Banku Centralnego.

Tomasz Buszkiewicz

udzie powinni móc swobodnie inwestować swoje pieniądze wszędzie tam, gdzie chcą – przyznała w jednym z wywiadów. – *Mogą spekulować, jeśli chcą. Ale nie powinni mieć swobody uczestniczenia w działalności objętej sankcjami kryminalnymi.*

Każde jej publiczne wystąpienie – nie tylko wtedy, gdy staje w twardej opozycji wobec rynku kryptowalut – jest wydarzeniem. To niekwestionowana gwiazda światowych finansów. Autokratyczna i egocentryczna, jak twierdzą pracownicy EBC, którzy oceniają swoją szefową w corocznych ankietach. Europejski Bank Centralny jest dla niej – stwierdzili w tegorocznym badaniu – a nie ona dla EBC.

Kim jest pierwsza kobieta na stanowisku szefa EBC?

Wybitna francuska polityczka i prawniczka, z doświadczeniem w kierowaniu resortami ekonomii, finansów i przemysłu, a także handlu zagranicznego, rolnictwa i rybołówstwa. Te bogate doświadczenia w kierowaniu różnymi sektorami w gospodarce realnej dają silne podstawy do kompetentnego podchodzenia do problemów polityki pieniężnej w strefie euro – twierdzi prof. nauk ekonomicznych Jan Szambelańczyk z Uniwersytetu WSB Merito Poznań.

Christine Lagarde to francuska ekonomistka i polityczka. Przed objęciem funkcji szefowej EBC zyskała szerokie uznanie jako minister finansów Francji oraz jako szefowa Międzynarodowego Funduszu Walutowego.

Swoją karierę zawodową Lagarde rozpoczęła w roli prawniczki, specjalizując się w sprawach korporacyjnych i antytrustowych. Z czasem przeszła do sektora finansowego, gdzie zdobyła doświadczenie w dziedzinie prawa bankowego i korporacyjnego. Jej talent i determinacja pozwoliły szybko awansować, co zaowocowało objęciem stanowiska ministra finansów Francji w rządzie Nicolasa Sarkozy'ego.

Jako minister finansów, Lagarde odgrywała kluczową rolę w zarządzaniu kryzysem finansowym w latach 2008-2009 oraz w walce z konsekwencjami tego kryzysu dla gospodarki francuskiej. Jej determinacja i umiejętność negocjacji przyczyniły się do osiągnięcia sukcesów w działaniach na rzecz stabilności finansowej i fiskalnej Francji.

Po odejściu z rządu, Lagarde objęła stanowisko dyrektora zarządzającego MFW, gdzie kontynuowała swoją pracę na rzecz stabilności finansowej i rozwoju gospodarczego na skalę globalną. Jej przywództwo w MFW było określane jako skuteczne i innowacyjne, przynosząc korzyści dla wielu krajów, szczególnie tych znajdujących się w trudnej sytuacji finansowej.

W 2019 roku Lagarde została wybrana na stanowisko szefowej Europejskiego Banku Centralnego. Jej podejście do polityki monetarnej jest często opisywane jako pragmatyczne i elastyczne, co pozwala skutecznie reagować na zmieniające się warunki gospodarcze i wyzwania finansowe.

Jednym z przykładów innowacyjności Christine Lagarde w roli lidera MFW był jej stanowczy nacisk na promowanie równości płci i zaangażowania społecznego w programach rozwoju gospodarczego. Lagarde konsekwentnie podkreśla, że równość płci ma kluczowe znaczenie dla wzrostu gospodarczego i redukcji ubóstwa. Podczas pracy w MFW promowała politykę, która uwzględniała płeć jako istotny czynnik w podejmowaniu decyzji makroekonomicznych, zachęcając państwa członkowskie do wdrażania programów mających na celu poprawę sytuacji kobiet na rynku pracy, dostęp do edukacji i finansowania, a także równego uczestnictwa w życiu gospodarczym. Działania Lagarde przyczyniły się do zwiększenia uwagi poświęcanej kwestiom równości płci w dyskusjach na temat rozwoju gospodarczego oraz do większego zaangażowania społeczności międzynarodowej w promowanie równych szans dla wszystkich.

Jako minister finansów, Lagarde odgrywała kluczową rolę w zarządzaniu kryzysem finansowym w latach 2008-2009 oraz w walce z konsekwencjami tego kryzysu dla gospodarki francuskiej.

FOT. WIKIPEDIA

Plotki głoszą, że radziła się magicznej 8-Kuli

Natomiast z czasów jej kierowania MFW pochodzą plotki, że gdy stawała przed skomplikowanymi dylematami decyzyjnymi korzystała z magicznej 8-Kuli, która potrząsana dawała jej pytyjskie porady od „Perspektywy są niejasne...” po „Zapytaj ponownie później...”, a te pomagały kierować polityką MFW. Wszystkie te plotki są oficjalnie dementowane – komentuje prof. Szambelańczyk.

Christine Lagarde hołduje zasadzie „trzech P”, którą często przywołuje w kontekście zrównoważonego rozwoju gospodarczego. Według tej zasady trzy P oznaczają: „People, Planet, Profit”, czyli ludzi, planetę i zysk. Szefowa EBC odnosi się w ten sposób do konieczności uwzględnienia równocześnie aspektów społecznych, środowiskowych i ekonomicznych w podejmowaniu decyzji gospodarczych. Ta prosta, ale zwięzła zasada odzwierciedla podejście Lagarde do budowania gospodarek opartych na zrównoważonym wzroście, w których równowaga między potrzebami ludzi, ochroną środowiska a osiąganiem zysków jest kluczowa dla długoterminowego sukcesu.

Anegdoty na temat Christine Lagarde często podkreślają jej determinację, dyplomację i charyzmę osobistą. Jedna z nich mówi, że kiedy została zapytana, jak radzi sobie z presją, odpowiedziała: „Zawsze noszę wysokie obcasy. One mnie podtrzymują”.

Plotka głosi, że czasami komunikuje się z monetami i banknotami euro, które udzielają jej mądrych rad na temat stóp procentowych i kursów. Niektórzy twierdzą wręcz, że nawet szepcze miłe słówka do banknotów 500 euro, namawiając je do swobodniejszej cyrkulacji. Podobnie mówi się, że ma tajemny skarbiec, w którym przechowuje wyrzucone i zgniecione paragony za wypitą kawę, które są rzekomo kluczem do stabilizacji światowej gospodarki – uśmiecha się profesor Szambelańczyk.

> Podczas pracy w MFW promowała politykę, która uwzględniała płeć jako istotny czynnik w podejmowaniu decyzji makroekonomicznych.

Portal Politico, który dotarł do wyników wspomnianej na wstępie ankiety oceniającej szefową EBC, podkreśla, że pracownicy banku krytykują Lagarde za nazbyt intensywne zaangażowanie w politykę i wykorzystywanie banku do realizacji własnych celów. Niewiele ponad jedna trzecia ankietowanych uważa, że decyzje Christine Lagarde dotyczące polityki pieniężnej były właściwe. Ponad połowa z nich utrzymuje, że Europejski Bank Centralny nie będzie w stanie zapewnić powrotu do stabilności cen, doprowadzając tym samym do inflacji znacznie powyżej celu inflacyjnego na rok 2024.

Pani Lagarde potrafi być kontrowersyjna

Interesujące są też refleksje pracowników na temat sposobu zarządzania personelem w EBC. Gwiazda światowych finansów – tak wnikliwie słuchana przez polityków na wszystkich kontynentach – pozwala na nadmierne obciążenie pracą i podwójne standardy w relacjach z personelem. Lagarde obrywa się za to, że zachęca do wewnętrznych „burz mózgów” i dzielenia się obawami, a następnie… krytykuje pracowników za nazbyt szczere opinie.

Płynące z EBC negatywne oceny działalności Christine Lagarde tylko potwierdzają tezę, że rola lidera nie polega wyłącznie na identyfikowaniu globalnych wyzwań i podejmowaniu strategicznych decyzji. Ważne, by być wrażliwym na potrzeby i opinie własnych współpracowników, posiadać umiejętność otwartego reagowania na wewnętrzną krytykę.

Przykład Lagarde pokazuje też, że prawdziwy lider jest w stanie zrozumieć, iż wzrost i rozwój organizacji zaczyna się od szacunku dla tych, którzy wspólnie budują jej fundamenty. Prawdziwa siła przywództwa tkwi bowiem w umiejętności balansowania pomiędzy widokiem na horyzoncie globalnych wyzwań, a troską o dobro i harmonię wewnątrz własnej społeczności. ●

CHRISTINE LEGARDE – ŻELAZNA DAMA EUROPEJSKICH FINANSÓW

W przeszłości była szefem dużej amerykańskiej kancelarii prawnej Baker & McKenzie, ministrem handlu, rolnictwa, gospodarki i finansów Francji. W latach 2011-2019 dwukrotnie pełniła funkcję dyrektor generalnej Międzynarodowego Funduszu Walutowego zajmującego się wspieraniem reform w krajach rozwijających się. Od 2019 r. pełni funkcję prezesa Europejskiego Banku Centralnego - najważniejszego banku strefy euro i obok amerykańskiego Systemu Rezerwy Federalnej uważanego za najważniejszy bank centralny na świecie, których decyzje śledzą rynki finansowe i banki centralne na całym globie. Z wykształcenia jest prawniczką, specjalizującą się w prawie pracy i fuzjach oraz przejęciach. Posiada ogromne zdolności negocjacyjne zdobyte podczas piastowania wielu ważnych funkcji. Podczas szczytów G7, G8 i G20 pełniła funkcję „szerpy", który uzgadnia teksty komunikatów i zawsze potrafiła postawić na swoim. Była zwolenniczką spłaty długów przez Grecję. Legarde pełniąc funkcję prezesa EBC była zwolennikiem pobudzania gospodarki tanim pieniądzem – przez co kontynuowała, w kryzysie pandemicznym (2020-2021) realizowany po globalnym kryzysie finansowym (2009-2013) przez jej poprzednika Mario Draghiego program luzowania ilościowego (QE, *quantitative easing*), czyli skup na rynku wtórnym od banków komercyjnych długoterminowych aktywów na dużą skalę, długoterminowych skarbowych papierów wartościowych (10-letnie obligacje rządu), który w krótkim horyzoncie zwiększał płynność w gospodarce, a w długim okresie doprowadził do powstania dużej inflacji w strefie euro. W związku z tym w 2023 r. konieczne było wdrożenie programu zacieśniania ilościowego (QT, *quantitative tightening*) o wartości 5 bln euro, będącego odwrotnością luzowania ilościowego. Jest przeciwnikiem ostrych regulacji w sektorze bankowym, bo jej zdaniem doprowadzą one do ucieczki kapitału do innych krajów.

Dr hab. Krzysztof Waliszewski, Uniwersytet Ekonomiczny w Poznaniu

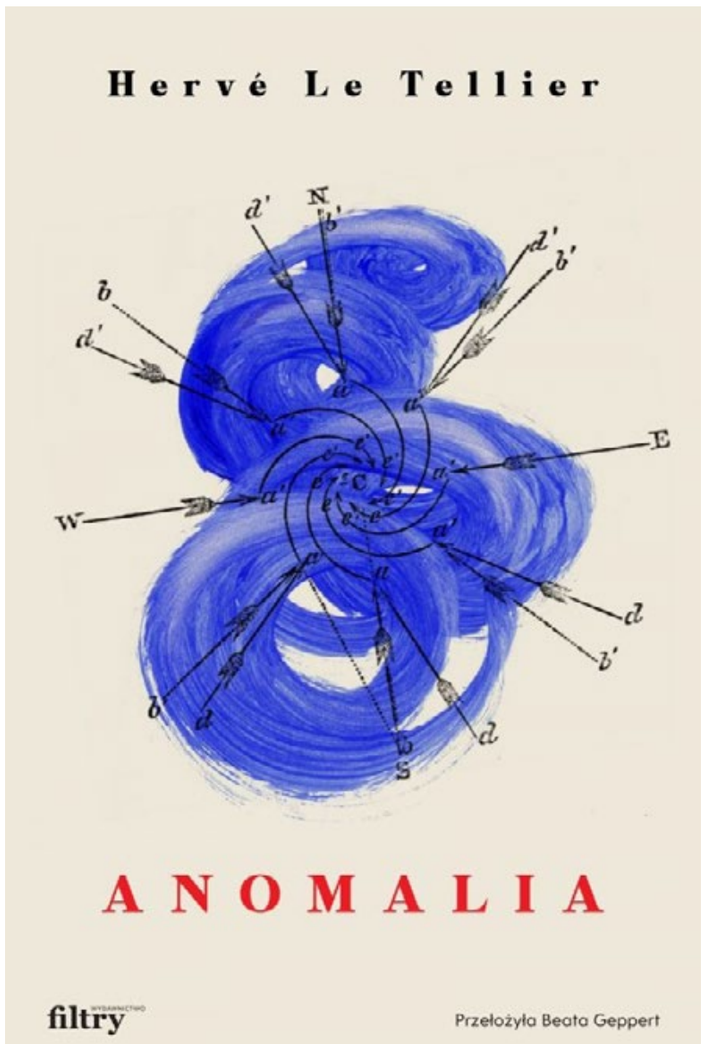
TROCHĘ KULTURY

Hervé Le Tellier „Anomalia”
Polski przekład: Beata Geppert

RAFAŁ ŁOPKA, SGB-BANK SA

„Anomalia” to świetnie napisana książka, wobec której ciężko przejść obojętnie. Powieść łączy w sobie elementy thrillera, powieści obyczajowej, SF czy dramatu. To książka, która zostawia czytelnika z ważnymi pytaniami o kondycję ludzkości, religię, filozofię czy politykę. Autor pisze jednak przystępnym językiem, zgrabnie bawi się gatunkami, chociaż nie stroni też od wątków erudycyjnych. Wszystko to okraszone jest specyficznym humorem, którego jest sporo, zwłaszcza w pierwszej części powieści.

Hervé Le Tellier jest członkiem hermetycznej grupy OuLiPo, która przemyca do tekstów literackich elementy logiki, matematyki czy teorii gier. Ale spokojnie, niech Was to nie zniechęca, często jest to po prostu gra z konwencjami literatury, pisanie według z góry przyjętych reguł. W tym przypadku mamy do czynienia z łagodnym przejściem z hermetycznej literatury w stronę dzieła otwartego dla szerokiej publiczności, pełnego odwołań



do współczesnych utworów literackich czy filmowych.

Informacje o autorze – bardziej szczegółowe oczywiście – podane są dopiero na końcu książki. Wcześniej mamy do czynienia z wielowątkową, wielonarracyjną opowieścią… właśnie, o czym?

Bardzo ciężko napisać coś więcej, żeby nie zaspojlerować. A to ważne, bo zwrocity akcji – zwłaszcza ten główny – świadczą m.in. o sile tej książki. Dlatego też nie spoglądajcie w ogóle na blurb na okładce – zepsuje Wam tylko zabawę.

Powieść rozpoczyna się od krótkich rozdziałów, w których poznajemy losy wielu osób, pozornie niezwiązanych ze sobą. Później z tego pozornego chaosu wyłania się zgrabna konstrukcja, w której bohaterowie (jest ich wielu, na pewno poczujecie sympatię do któregoś z nich) muszą się zmierzyć z trudnymi wyborami i relacjami międzyludzkimi. W tle pewien feralny lot Paryż–Nowy Jork, rządy mocarstwowych państw, ich prezydenci i doradcy/doradczynie.

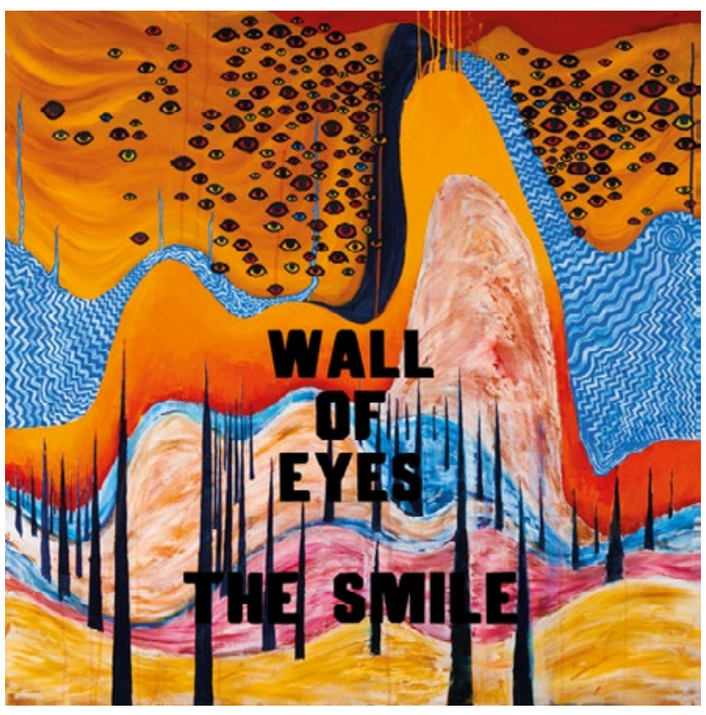
Kiedy wątki zaczną się ze sobą łączyć, już będzie po Was – przepadliście. W tej książce nic nie jest przypadkowe. Autor wciągnie Was w swój alternatywny świat i poprowadzi po sznurku prosto do odpowiedzi na jedno, bardzo ważne pytanie. Tak, wiem, teraz może nie mieć ono sensu, po przeczytaniu książki zapewniam, że będzie miało:

Co zrobił(a)byś, będąc… na swoim miejscu? :) ●

The Smile – Wall of Eyes
XL Recordings 2024

JĘDRZEJ SZYMANOWSKI, SGB-BANK SA

Zarówno słuchacze, jak i zawodowi komentatorzy muzyki, zgodnie określają Radiohead mianem najważniejszego zespołu ostatniego ćwierćwiecza. Od gitarowego britpopu w latach dziewięćdziesiątych, przez eksperymenty z elektroniką na przełomie wieków, po coraz to bardziej wymykające się szufladkom międzygatunkowe flirty z ostatnich lat. Szeregiem coraz to bardziej bezkompromisowych innowacji na przestrzeni dekad wypracowali markę samą w sobie. Brytyjczycy mają swój własny świat, do którego co jakiś czas zapraszają tych, którzy nie boją się, że w rockowym utworze zbije ich z pantałyku wstawka rodem z muzyki partyturowej lub ambientowa plama. I choć od 8 lat nie wydali nowej płyty, członkom Radiohead trudno powstrzymać się od prezentacji nowych pomysłów szerokiej publiczności – stąd projekty poboczne. Jednym z nich jest The Smile – formacja, która skupia całą siłę kreatywną macierzystego zespołu, czyli Thoma Yorke’a i Jonny’ego Greenwooda. Obaj są wszech-



stronnymi muzykami i kompozytorami o ogromnej erudycji, w największej mierze odpowiedzialnymi za wyjątkowy styl „radiogłowych”. Nic dziwnego, że The Smile określa się czasem po prostu „tym drugim Radiohead”. Przygrywa im tu Tom Skinner – perkusista jazzowego Sons of Kemet, którego bogata gra znacząco poszerza kapitał kulturowy grupy. „Wall of Eyes” to ich drugi wspólny album, po wydanym dwa lata temu debiucie (choć – przyznajmy – debiutantami nazwać ich ciężko). Płytę wypełniają wprawdzie piosenki, ale zazwyczaj ugryzione w dość nietypowy sposób. Na początek leci ładny utwór w estetyce bossa novy, który stopniowo przeobraża się w paranoiczny pejzaż wokalnych ścinek, niepokojących orkiestracji i drobnych gitarowych udziwnień. I tak już będzie właściwie przez całe 45 minut. Utwory na „Wall of Eyes” mają piękne i wyraziste melodie, jednak daleko im do standardowych struktur piosenkowych. To nieprzerwanie transmutujące, wielosegmentowe projekty o zmiennych podziałach rytmicznych – szczególnie słychać to w suitach „Under Our Pillows” i „Bending Hectic”. Ten pierwszy zaczyna się matematyczną gitarą rodem z King Crimson, by z czasem przeprowadzić nas przez pędzący krautrockowy motorik, aż do wyciszenia awangardową muzyką tła. Drugi to z kolei osiem minut przygody – od mrocznego folku w manierze Tima Buckleya, przez afrobeat, po przesterowane rockowe wyładowanie, do którego prowadzi symfoniczne crescendo (na całym krążku produkuje się London Contemporary Orchestra). Fani „tego pierwszego Radiohead” powinni się (nomen omen) uśmiechnąć – szczególnie jeśli przypadły im do gustu ostatnie albumy Yorke’a i spółki. ●

Biedne Istoty

Film4 Productions, Element Pictures, TSG Entertainment i Searchlight Picture

MACIEJ KARWOWSKI, SGB-BANK SA

W tym miejscu miała znajdować się recenzja drugiej części „Diuny” – wielkiego, ambitnego projektu Denisa Villeneuve’a opartego na podstawie powieści Franka Herberta. Niestety, pokonała mnie polska widownia. Widownia spragniona, tak jak ja, obejrzenia tego filmu w jedynym słusznym formacie – Imaxie. Wszystkie pokazy na wiele dni do przodu pękają w szwach, zmuszając mnie do odłożenia seansu na później. W końcu wielkie dzieła wymagają wielkich ekranów, prawda? Niekoniecznie.

Wie to każdy, kto już widział najnowszy film Yórgosa Lánthimosa „Biedne istoty”. Choć i tu nie brak efektów specjalnych oraz zdecydowanie jest na czym oko zawiesić – a za wszystkie te elementy słusznie obraz zgarnął łącznie cztery Oscary (kostiumy, scenografia, charakteryzacja, Emma Stone) – to jest to tytuł zgoła odmienny od pustynnej epopei kanadyjskiego twórcy. Ale w mym poczuciu znacznie bardziej interesujący.

Lánthimosowi udaje się rzecz niesłychana – tworząc ambitne, nieoczywiste kino, jest w stanie zainteresować nim szerszą publikę. Tyczy się to przede wszystkim poprzedniej „Faworyty” i właśnie „Biednych istot”. Czy decydującym elementem tej układanki jest Emma Stone, w obu produkcjach obsadzona w roli głównej? Być może. Albowiem jest to aktorka, nie boję się użyć tego słowa, wybitna, która udowodniła kreacjami m.in. w „Służących”, „La la land” czy „Birdmanie”, że dołoży wszelkich starań, by zapisać się w historii kina złotymi zgłoskami.

Myśl ta przyświeca i samemu reżyserowi, który stworzył film bardzo nietuzinkowy i hipnotyzujący. Oto dziwaczny, alternatywny świat początku XX wieku, w którym to Godwin Baxter (w tej roli William Dafoe), naukowiec o mało moralnych pobudkach, tworzy swojego potwora Frankensteina – Bellę Baxter, człowieka o ciele dorosłej kobiety, a umyśle jej nienarodzonego dziecka. Brzmi dziwnie, ale intrygująco? Dokładnie takie jest.

Przez blisko dwie i pół godziny metrażu dane nam jest oglądać dorastanie Belli, jej poznawanie świata, mierzenie się z prawidłami nim rządzącymi oraz jej emancypację. Lánthimosowi jednak ewidentnie nie zależy na wpisaniu się w obecne feministyczne trendy. U niego dzieje się to organicznie i wynika ze zrozumienia swoich postaci – ich dramatów i potrzeb. Ciekawy pod tym względem jest również aspekt seksualny życia bohaterki. „Biedne istoty” przepełnione są różnorakimi scenami seksu, jednak w żadnej z tych sytuacji Stone nie jest seksualizowana. Jasnym jest dlaczego oglądamy te sceny i co ma z nich wynikać. To kreowana postać ma być podniecona, a nie widz. Potwierdzeniem takiego podejścia są wypowiedzi aktorki na temat pracy na planie. Kobieta czuła się na planie komfortowo, a nie jako obiekt seksualny? W starym Hollywood byłoby to nie do pomyślenia.

Choć niewątpliwie „Biedne istoty” to film udany i godny zobaczenia, nie mogę go polecić każdemu. Świat wykreowany na ekranie jest dziwaczny i surrealistyczny, skrzekliwa muzyka niejednego przyprawi o ból głowy, a od przepychu scenograficznego można dostać oczopląsu. Jednak może warto czasem wyjść ze swojej strefy komfortu, by przekonać się, jak dziś wygląda sztuka filmowa? Może wszyscy jesteśmy biednymi istotami, a taki seans może nas tylko ubogacić. ●

WYKONYWANIE CZYNNOŚCI MAKLERSKICH BEZ PROWADZENIA DZIAŁALNOŚCI MAKLERSKIEJ

Adam Karmoliński

Jan Solarski

SMM Legal Maciak Mataczyński Czech Sp.K. z siedzibą w Warszawie

Działalność maklerska

Działalność maklerska jest działalnością ściśle regulowaną oraz nadzorowaną. Podjęcie oraz późniejsze jej prowadzenie, zgodnie z art. 69 ust. 1 w zw. z art. 82 u.o.i.f. oraz na podstawie art. 111 ust. 1 u.o.i.f., wymaga stałego posiadania przez podmiot podejmujący i prowadzący tę działalność odpowiedniego zezwolenia administracyjnego[1]. Tym samym ustawodawca krajowy wprowadził ogólny zakaz podejmowania i prowadzenia działalności maklerskiej przez podmioty niedysponujące odpowiednim zezwoleniem. Na dowód tego, że działalność maklerska cechuje się znacznym stopniem zaawansowania oraz fachowości, ale także celem dbania o interesy klientów (co wydaje się jest zadaniem nadrzędnym), podjęcie i prowadzenie takiej działalności przez podmiot, który nie dysponuje wymaganym zezwoleniem lub upoważnieniem, zagrożone jest odpowiedzialnością karną[2]. Ratio legis wprowadzenia takiego rozwiązania pozostaje właśnie zapewnienie odpowiedniego poziomu ochrony podmiotom korzystającym z usług maklerskich i odpowiedniego poziomu profesjonalizmu podmiotów, które podejmują i prowadzą działalność maklerską[3].

Podmiotami, z którymi w polskich realiach klienci najczęściej utożsamiają prowadzenie działalności maklerskiej oraz z drugiej strony – z których usług w zakresie wykonywania czynności maklerskich chętnie korzystają, są domy i biura[4] maklerskie. Podejście to wydaje się uzasadnione, gdyż poprzez firmę inwestycyjną – podmiot, do którego w głównej mierze adresowane są obowiązki określone w u.o.i.f. od strony regulacyjnej, rozumie się przede wszystkim dom maklerski. Nie jest to jednak jedyny podmiot, który według ustawodawcy krajowego może określać się mianem firmy inwestycyjnej i dzięki temu oferować określone usługi maklerskie. Oprócz domu maklerskiego, na podstawie art. 3 pkt 33 u.o.i.f., firma inwestycyjna oznacza także bank prowadzący działalność maklerską (w formie wspomnianego biura maklerskiego), zagraniczną firmę inwestycyjną prowadzącą działalność maklerską na terytorium Rzeczypospolitej Polskiej oraz zagraniczną osobę prawną z siedzibą na terytorium państwa innego niż państwo członkowskie, prowadzącą na terytorium Rzeczypospolitej Polskiej działalność maklerską.

Wykonywanie czynności maklerskich na podstawie wyjątku

Dla celów niniejszego artykułu najistotniejsza pozostaje jednak treść przepisu art. 70 ust. 2 u.o.i.f, zgodnie z którym bank z siedzibą na terytorium Rzeczypospolitej Polskiej może, poza jednostką wydzieloną organizacyjnie (w rozumieniu art. 111 ust. 5 u.o.i.f.), wykonywać czynności maklerskie w zakresie

---

[1] Zob. art. 69 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j. Dz.U. z 2023 r. poz. 646 z późn. zm.) (u.o.i.f.), który stanowi, że prowadzenie działalności maklerskiej wymaga zezwolenia Komisji wydanego na wniosek, o którym mowa w art. 82, złożony przez zainteresowany podmiot. Art. 82 u.o.i.f. określa z kolei dokładne warunki składania wniosku o dzielenie zezwolenia na prowadzenie działalności maklerskiej przez podmiot nieposiadający statusu domu maklerskiego. Art. 111 u.o.i.f. opisuje natomiast wymogi formalne dla złożenia wniosku o prowadzenie działalności maklerskiej przez bank z siedzibą na terytorium Rzeczypospolitej Polskiej.

[2] Zob. art. 178 u.o.i.f., który stanowi, że kto bez wymaganego zezwolenia lub upoważnienia zawartego w odrębnych przepisach albo nie będąc do tego uprawnionym w inny sposób określony w ustawie, prowadzi działalność w zakresie obrotu instrumentami finansowymi, podlega grzywnie do 5 000 000 zł albo karze pozbawienia wolności do lat 5, albo obu tym karom łącznie.

[3] P. Wajda [w:] M. Wierzbowski, L. Sobolewski, P. Wajda (red), Ustawa o obrocie instrumentami finansowymi. Komentarz Prawo rynku kapitałowego. Tom I–II, Warszawa 2023, Legalis.

[4] Zgodnie z § 2 pkt 4 Rozporządzenia Ministra Finansów z dnia 29 maja 2018 r. w sprawie szczegółowych warunków technicznych i organizacyjnych dla firm inwestycyjnych, banków, o których mowa w art. 70 ust. 2 ustawy o obrocie instrumentami finansowymi, i banków powierniczych (Dz.U. z 2018 r. poz. 1111 z późn. zm.), przez biuro maklerskie rozumie się oddział lub inną jednostkę banku prowadzącego działalność maklerską działającą na zasadach oddziału, wyodrębnioną organizacyjnie, w ramach której bank prowadzi tę działalność.

określonym u.o.i.f. Ustawodawca, na podstawie art. 70 ust. 2 u.o.i.f., zwalnia zatem bank (krajowy) z obowiązku uzyskania zezwolenia na prowadzenie działalności maklerskiej.

Dla banku działającego w trybie art. 70 ust. 2 u.o.i.f. nie jest też wymagane organizacyjne wydzielenie takiej działalności w ramach jego struktur bankowych[5]. Konsekwencją powyższego jest fakt, że działalność banku w trybie art. 70 ust. 2 u.o.i.f., nie jest, na podstawie art. 70 ust. 3 u.o.i.f., działalnością maklerską podstawową (czyli taką, o której stanowi art. 69 ust. 2 u.o.i.f.). Tym samym banki mogą bez zezwolenia na prowadzenie działalności maklerskiej wykonywać czynności ściśle wskazane w art. 70 ust. 2 u.o.i.f. Taki tryb wykonywania określonych czynności ma charakter autonomiczny i opiera się na wyrażonym explicite w art. 70 ust. 3 w zw. z ust. 2 u.o.i.f. wyłączeniu spod reżimu monopolu maklerskiego, adresowanym tylko do banków[6]. Banki, w trybie art. 70 ust. 2 u.o.i.f., mogą świadczyć wyłącznie (jest to katalog zamknięty) czynności mieszczące się w czynnościach maklerskich *sensu stricto* określone w:

1) art. 69 ust. 2 pkt 1, 2 *(przyjmowanie i przekazywanie zleceń nabycia lub zbycia instrumentów finansowych, w tym na rachunek dającego zlecenie) i 4-6 (zarządzanie portfelami, w skład których wchodzi jeden lub większa liczba instrumentów finansowych; doradztwo inwestycyjne; oferowanie instrumentów finansowych)* – o ile przedmiotem tych czynności są papiery wartościowe, o których mowa w art. 4 ust. 1 pkt 2 u.o.i.f., lub inne niedopuszczone do obrotu zorganizowanego instrumenty finansowe, obligacje emitowane przez Bank Gospodarstwa Krajowego na rzecz funduszy utworzonych, powierzonych albo przekazanych temu bankowi na podstawie odrębnych ustaw, gwarantowane przez Skarb Państwa, a także obligacje emitowane przez Bankowy Fundusz Gwarancyjny lub podmiot zarządzający aktywami, o którym mowa w art. 224 ust. 1 ustawy z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji;
2) art. 69 ust. 2 pkt 7 *(świadczenie usług w wykonaniu zawartych umów o gwarancję emisji lub zawieranie i wykonywanie innych umów o podobnym charakterze, jeżeli ich przedmiotem są instrumenty finansowe)*;
3) art. 69 ust. 2 pkt 3 *(nabywanie lub zbywanie na własny rachunek instrumentów finansowych)* – jeżeli nie są one wykonywane w ramach pełnienia funkcji animatora rynku na akcjach lub instrumentach pochodnych, których instrumentem bazowym są akcje;
4) art. 69 ust. 4^7 – jeżeli wykonuje co najmniej jedną z czynności, o których mowa w pkt 1-3 lub 5;
5) art. 69 ust. 2 pkt 1 i 2 *(przyjmowanie i przekazywanie zleceń nabycia lub zbycia instrumentów finansowych, w tym na rachunek dającego zlecenie)* – jeżeli przedmiotem tych czynności jest pośredniczenie w zawieraniu transakcji pożyczek papierów wartościowych w rozumieniu art. 3 pkt 7 rozporządzenia 2015/2365, przez przyjmowanie i przekazywanie zleceń dotyczących pożyczek papierów wartościowych, zawieranie transakcji pożyczek papierów wartościowych w imieniu własnym i na rzecz dającego zlecenie albo w imieniu i na rzecz dającego zlecenie, jeżeli przedmiotem tych transakcji są papiery wartościowe dopuszczone do obrotu zorganizowanego.

> Tym samym ustawodawca krajowy wprowadził ogólny zakaz podejmowania i prowadzenia działalności maklerskiej przez podmioty niedysponujące odpowiednim zezwoleniem.

Co istotne, zwolnienie przez ustawodawcę banków wykonujących czynności w trybie art. 70 ust. 2 u.o.i.f. z wymogu uzyskania zezwolenia nie oznacza *in extenso* wyjęcia wykonywania tych czynności spod reżimu u.o.i.f.[8], o czym świadczy art. 70 ust. 4 u.o.i.f., zgodnie z którym do banku korzystającego z opisywanego wyjątku i wykonującego określone powyżej czynności stosuje się przepisy nakładające na bank m.in. obowiązek zawarcia „umowy o świadczenie usług brokerskich" (art. 73 u.o.i.f.), obowiązek starannego działania na rzecz klienta (art. 73a u.o.i.f.), obowiązek wdrożenia polityki wykonywania zleceń (art. 73b u.o.i.f.) czy chociażby obowiązek uzyskania od klienta adekwatnej wiedzy dotyczącej jego wiedzy i doświadczenia w zakresie inwestowania na rynku finansowym, sytuacji finansowej oraz celów inwestycyjnych (art. 83g u.o.i.f.).

Pomimo, że bank chcący wykonywać określone czynności maklerskie nie musi dopełniać tylu formalności, ilu oczekuje się od podmiotu składającego wniosek o wydanie zezwolenia na prowadzenie działalności maklerskiej, świadczenie usług w trybie art. 70 ust. 2 u.o.i.f. wiąże się z licznymi obowiązkami, mającymi na celu zapewnić bezpieczeństwo oraz komfort klientom. Zabezpieczenie interesów klientów jest bowiem postrzegane przez ustawodawcę jako kluczowe dobro, bez którego rozwój rynku finansowego w Polsce nie byłby możliwy, czego przejawem może być m.in. obowiązek członkostwa w systemie rekompensat prowadzonym przez Krajowy Depozyt Papierów Wartościowych (KDPW). Więc pomimo że korzystanie z usług maklerskich zawsze wiąże się z pewnym ryzykiem, zarówno ustawodawca, jak i firmy inwestycyjne starają się dokładać wszelkich starań, by świadczone przez nich usługi gwarantowały komfort i bezpieczeństwo rywalizując w tym zakresie o zainteresowanie klienta. ●

---

[5] Jak np. w przypadku art. 111 ust. 5 u.o.i.f., który stanowi, że bank może prowadzić działalność maklerską pod warunkiem, że działalność ta jest organizacyjnie wyodrębniona od pozostałej działalności banku (wydzielenie organizacyjne).

[6] M. Michalski, Ramy prawne działalności inwestycyjnej banków w świetle dyrektywy 2004/39/WE oraz przepisów prawa polskiego, Monitor Prawniczy 2010, nr 24.

[7] Działalnością maklerską jest również wykonywanie przez firmę inwestycyjną czynności polegających na: (i) przechowywaniu lub rejestrowaniu instrumentów finansowych, w tym prowadzeniu rachunków papierów wartościowych, rachunków derywatów i rachunków zbiorczych oraz prowadzeniu rachunków pieniężnych, a także prowadzeniu ewidencji instrumentów finansowych; (ii) udzielaniu pożyczek pieniężnych w celu dokonania transakcji, której przedmiotem jest jeden lub większa liczba instrumentów finansowych, jeżeli transakcja ma być dokonana za pośrednictwem firmy inwestycyjnej udzielającej pożyczki; (iii) doradztwie dla przedsiębiorstw w zakresie struktury kapitałowej, strategii przedsiębiorstwa lub innych zagadnień związanych z taką strukturą lub strategią; (iv) doradztwie i innych usługach w zakresie łączenia, podziału oraz przejmowania przedsiębiorstw; (v) wymianie walutowej, w przypadku gdy jest to związane z działalnością maklerską w zakresie wskazanym w ust. 2; (vi) sporządzaniu analiz inwestycyjnych, analiz finansowych oraz innych rekomendacji o charakterze ogólnym dotyczących transakcji w zakresie instrumentów finansowych; (vii) świadczeniu usług dodatkowych związanych z umową o gwarancję emisji; (viii) wykonywaniu czynności określonych w pkt 1-7 oraz w ust. 2, których przedmiotem są instrumenty bazowe instrumentów pochodnych, wskazanych w art. 2 ust. 1 pkt 2 lit. d-f oraz i, jeżeli czynności te pozostają w związku z działalnością maklerską.

[8] M. Burzyńska, 5. Kredyt walutowy – wielkie nieporozumienie [w:] Problemy współczesnej bankowości, red. W. Góralczyk, Warszawa 2014.

CO NA TAPECIE W SPORACH KLIENTÓW Z BANKAMI?

Z Weroniką Magdziak-Śliwą, adwokatką i Partnerem w praktyce Sporów Instytucji Finansowych kancelarii Kochański & Partners rozmawia Robert Azembski

Na początek kwestia już nie nowa, lecz ważna, tj. podważania umów kredytowych złotowych opartych o WIBOR. Z jakimi przypadkami mamy obecnie do czynienia? Czy można powiedzieć już o jakimś „umasowieniu się" tego rodzaju praktyki oraz jaka jest dominująca linia orzecznicza w tej kwestii?

Problematyka sporów na tle umów kredytowych opartych o WIBOR wykształciła pewną praktykę w zakresie podstaw roszczeń formułowanych przez kredytobiorców. Obecnie ukształtowały się dwie główne grupy zarzutów kierowanych wobec tego rodzaju umów. Pierwsza to zarzuty dotyczące wadliwości mechanizmu funkcjonowania wskaźnika WIBOR, które wskazują na podatność wskaźnika na manipulacje, jego brak reprezentatywności – fikcyjność transakcji, jak również udział samych banków w procesie wyznaczania jego wysokości.

Drugą grupę stanowią zarzuty dotyczące naruszenia przez banki obowiązków informacyjnych wobec kredytobiorców.

Spory te są bardzo medialne. Praktycznie każdy wydany wyrok udostępniony opinii publicznej opatrzony jest licznymi komentarzami, co może dawać złudne poczucie ich masowości. W praktyce jednak na koniec 2023 roku szacowano liczbę aktywnych sporów na tym tle na ok. kilkaset spraw, co przy liczbie aktywnych kredytów hipotecznych opartych o WIBOR szacowanych na ok. 2,3 mln jest liczbą znikomą. Przekłada się to również na niewielką liczbę prawomocnych rozstrzygnięć.

Truizmem jest więc stwierdzenie, iż orzecznictwo w tym zakresie dopiero się kształtuje. Podkreślić jednak należy, że obecnie pojawia się coraz więcej orzeczeń oddalających roszczenia kredytobiorców.

Czy banki powinny być już teraz przygotowane na próby podważania umów o kredyty oparte o stopę WIBOR czy WIRON? Jeśli tak, to w jaki sposób mogą tu kalkulować związane z nimi ryzyko prawne?

Na razie jest stanowczo zbyt wcześnie, aby mówić o jakiejkolwiek nieważności umów kredytowych opartych o wskaźnik WIBOR czy też nieważności samego wskaźnika WIBOR. Niemożliwa jest też obecnie ocena czy negatywne dla kredytobiorców orzeczenia skutecznie zniechęcą ich do składania kolejnych pozwów, czy też problematyka ta stanie się punktem wyjścia do składania masowych powództw skierowanych przeciwko bankom.

Nie sposób pominąć jednak faktu, iż kwestia ta nierozerwalnie związana jest z systemem ochrony konsumenckiej, który jest obecnie bardzo rozbudowany, a przez to również mniej przewidywalny. Wszystko to powoduje, że odpowiednie kalkulowanie ryzyka prawnego z tym związanego jest bardzo utrudnione.

Biorąc jednak pod uwagę skalę, a co za tym idzie skutki dla całego sektora finansowego oraz gospodarki, które mogłyby wiązać się z wyeliminowaniem wskaźnika WIBOR czy też WIRON z umów, niezwykle ważna jest kwestia zarządzania ryzykiem prawnym w kontekście reformy wskaźników referencyjnych. Świadomość zarzutów kierowanych przez kredytobiorców może pomóc wypracować mechanizmy, które ryzyka związane z aktualnie ukształtowanym reżimem ochrony konsumenckiej pozwolą ograniczyć. Kluczowe wydaje się być zwłaszcza odpowiednie dostosowanie regulacji związanych z obowiązkami informacyjnymi.

Niektóre kancelarie prawne reprezentujące klientów banków twierdzą, że wybrane umowy kredytów konsumenckich mogą zawierać wady pozwalające na uzyskanie tzw. sankcji kredytu darmowego, wynikającej z ustawy o kredycie konsumenckim. Jakie ryzyko może wiązać się z tym dla banku w relacji z klientem – kredytobiorcą?

Sankcja kredytu darmowego to rozwiązanie przyjęte przez polskiego ustawodawcę w ustawie z dnia 20 lipca 2001 r. o kredycie konsumenckim, a obecnie reguluje ją ustawa z dnia 12 maja 2011 roku o kredycie konsumenckim, będąca skutkiem implementacji do polskiego porządku prawnego dyrektywy 2008/48/WE. Istotą sankcji jest pozbawienie kredytodawcy

prawa do pobierania odsetek i innych kosztów kredytu należnych kredytodawcy w terminie i w sposób ustalony w umowie (z wyjątkiem opłat związanych z ustanowieniem zabezpieczenia i ubezpieczenia kredytu). Krótko mówiąc bank lub firma pożyczkowa nie zarobi nic na udzielonym kredycie lub pożyczce. Kredytobiorca zwraca wtedy jedynie kapitał. Jeżeli konsument takie odsetki lub koszty uprzednio zapłacił na rzecz kredytodawcy, w majątku konsumenta powstają roszczenia w stosunku do kredytodawcy o zwrot uiszczonych kwot. Sankcja kredytu darmowego nie powoduje wygaśnięcia po stronie konsumenta obowiązku zwrotu kapitału wykorzystanego kredytu na rzecz kredytodawcy. Konsument – co do zasady – zwraca taki kapitał w terminie i w sposób określony w umowie o kredyt konsumencki.

W ostatnim czasie zostały opublikowane dwa mogące zaniepokoić banki nowe wyroki TSUE (-755/22, NÁROKUJ S.R.O. PRZECIWKO EC FINANCIAL SERVICES, A.S. oraz drugi, wcześniejszy w sprawie C 303/20 Ultimo Portfolio Investment [Luxemburg] SA przeciwko kredytobiorcy będącemu osobą fizyczną).
Czy co do zasady brak ze strony banku właściwej oceny zdolności kredytowej klienta może stać się przyczynkiem do podważenia całej umowy kredytowej?

Obowiązek dokonania oceny zdolności kredytowej konsumenta przed zawarciem umowy o kredyt konsumencki wynika z art. 9 ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, implementującej do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady 2008/48/WE z dnia 23 kwietnia 2008 roku w sprawie umów o kredyt konsumencki oraz uchylającą dyrektywę Rady 87/102/EWG. Zgodnie z art. 23 tej dyrektywy państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszenia przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą i podejmują wszelkie niezbędne działania w celu zapewnienia stosowania tych sankcji. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. W polskim porządku prawnym brak jest norm, które wprowadzałyby sankcję nieważności umowy o kredyt konsumencki w przypadku naruszenia obowiązków związanych z oceną zdolności kredytowej konsumenta.
Z wyroku TSUE z dnia 10 czerwca 2021 r. w sprawie C-303/20 wynika, że sądy powinny dysponować zakresem uznania, pozwalającym im w okolicznościach konkretnego przypadku dobrać środek odpowiedni do wagi stwierdzonego uchybienia obowiązkowi.
Wysoce wątpliwym wydaje się, aby niewłaściwa ocena zdolności kredytowej mogła być podstawą do nieważności całej umowy, jednak wszystko zależy od okoliczności danej sprawy, w tym wagi naruszenia. Natomiast wyrok TSUE z dnia 11 stycznia 2024 r. w sprawie C 755/22 zapadł na gruncie ustawodawstwa czeskiego, zgodnie z którym za naruszenie obowiązków związanych z badaniem zdolności kredytowej, prawo przewiduje sankcję nieważności umowy.

W jakich sytuacjach i pod jakimi warunkami bank nie ponosi odpowiedzialności za nieświadomie popełnione błędy przez klientów skutkujące np. opróżnieniem rachunku ze zgromadzonych na nim środków (oszustwa typu na BLIK, klik itp.)?

W ostatnim czasie coraz więcej osób pada ofiarą cyberprzestępców, którzy stosują różne metody manipulacji. Nierzadko oszustom udaje się osiągnąć swój cel i dokonać kradzieży pieniędzy

z rachunku bankowego. Bank jako dostawca usług płatniczych pełni rolę gwaranta środków pieniężnych zgromadzonych na rachunkach bankowych. Co do zasady banki mają obowiązek niezwłocznego zwrotu kwoty transakcji, na którą płatnik nie wyraził zgody (nieautoryzowane transakcje), na podstawie ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (dalej: „UPP"). Banki mogą zwolnić się z obowiązku zwrotu pieniędzy. Muszą wówczas zaistnieć przesłanki, o jakich mowa w art. 46 ust. 3 UPP. W myśl tego przepisu płatnik odpowiada za nieautoryzowane transakcje płatnicze w pełnej wysokości, jeżeli doprowadził do nich umyślnie albo w wyniku umyślnego lub będącego skutkiem rażącego niedbalstwa naruszenia co najmniej jednego z obowiązków, o których mowa w art. 42 UPP (obowiązek korzystania z instrumentu płatniczego zgodnie z umową ramową oraz zgłaszania niezwłocznie dostawcy lub podmiotowi wskazanemu przez dostawcę stwierdzenie utraty, kradzieży, przywłaszczenia albo nieuprawnionego użycia instrumentu płatniczego lub nieuprawnionego dostępu do tego instrumentu).
Bank nie poniesie odpowiedzialności za kradzież z rachunku zgromadzonych w nim środków np. w sytuacji, gdy płatnik dobrowolnie udostępni osobie trzeciej na przykład login i hasło do logowania w systemie bankowości elektronicznej, bądź kartę płatniczą z numerem PIN.
Jeśli natomiast właściciel rachunku zostanie podstępnie skłoniony przez osobę nieuprawnioną do udostępnienia danych, odpowiedzialność banku będzie zależała od tego, czy płatnik zachował się w sposób rażąco niedbały. Przykładem takiego rażącego niedbalstwa może być sytuacja, w której płatnik padł ofiarą popularnego obecnie oszustwa i kliknął w link zawarte-

FOT. ARCHIWUM KANCELARII KOCHAŃSKI&PARTNERS

go w sms-ie o niedopłacie, np. za prąd, kierującego na stronę umożliwiającą wyłudzenie danych. Otrzymanie takiej wiadomości winno wzbudzić w płatniku, oceniając rozsądnie, podejrzenie co do prawdziwości danych tam zawartych i skłaniać do podjęcia kontaktu z dostawcą prądu celem wyjaśnienia sytuacji, szczególnie jeśli nigdy wcześniej takich wiadomości sms nie otrzymywał. Również zignorowanie komunikatów sms-owych z banku o dodaniu nowego urządzenia do autoryzacji, którego płatnik sam nie dodawał stanowi przejaw rażącego niedbalstwa. ●

ZASTRZEŻENIE NUMERU PESEL – NA CZYM POLEGA I CO OZNACZA DLA BANKÓW?

Anna Loch
SGB-Bank SA

Bogumiła Mendyk
SGB-Bank SA

Radosław Żmudziński
SGB-Bank SA

Ustawą z 7 lipca 2023 r. o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości[1] (dalej: „Ustawa") ustawodawca „wyposażył" osoby fizyczne w narzędzie, które ma zapobiegać negatywnym skutkom kradzieży tożsamości (jeśli zaistnieją w przyszłości) lub zmniejszyć ich uciążliwość (jeśli już nastąpiły). Zastrzeżenie numeru PESEL staje się niejako „bronią" do walki z negatywnymi skutkami powszechnego w ostatnich latach zjawiska kradzieży tożsamości. Czy zatem zastrzegając swój numer PESEL możemy czuć się bezpieczniej? Na to pytanie spróbujemy odpowiedzieć z punktu widzenia osoby fizycznej korzystającej z usług i produktów bankowych. Ale po kolei.

Ustawa posługuje się pojęciem zastrzeżenia numeru PESEL, które jest w istocie blokadą numeru PESEL, bowiem zastrzeżenie można w każdej chwili cofnąć. Zastrzeżenie nie prowadzi również do nadania nowego numeru PESEL. Polega wyłącznie na dokonaniu odpowiedniego wpisu w rejestrze zastrzeżeń numerów PESEL, prowadzonego przez ministra właściwego ds. informatyzacji w systemie teleinformatycznym.

KTO I JAK MOŻE GO DOKONAĆ?

Zastrzec numer PESEL może pełnoletnia osoba fizyczna posiadająca numer PESEL. Dotyczy to również cudzoziemców, którym został nadany numer PESEL. Zatem ustawodawca nie przewidział możliwości zastrzeżenia numeru PESEL osoby niepełnoletniej. Zastrzeżenie PESEL i jego cofnięcie jest nieodpłatne. Może być dokonane:

a) osobiście w organie dowolnej gminy (na wniosek);
b) przy użyciu usługi elektronicznej udostępnionej przez ministra właściwego ds. informatyzacji, po uwierzytelnieniu (np. w aplikacji mObywatel, poprzez ePUAP);
c) w placówce banku, SKOK czy wyznaczonego operatora pocztowego lub za pomocą systemu teleinformatycznego banku/SKOK (np. poprzez bankowość elektroniczną), pod warunkiem uprzedniego udostępnienia usługi zastrzeżenia numeru PESEL przez te podmioty; ale UWAGA: nie będzie możliwe cofnięcie zastrzeżenia w sposób opisany w tym punkcie.

Cofnięcia zastrzeżenia można dokonać bezterminowo albo określić datę i godzinę, kiedy system automatycznie zastrzeże numer PESEL. Nie można dokonać ponownego zgłoszenia zastrzeżenia PESEL przez 30 minut od jego cofnięcia.

WERYFIKACJA ZASTRZEŻENIA NUMERU PESEL PRZEZ BANKI

Od kiedy i w jakich przypadkach?

Dla banków obowiązek weryfikacji zastrzeżenia numeru PESEL w określonych w Ustawie przypadkach wchodzi w życie 1 czerwca 2024 r. Właściwie to dopiero od tego momentu zastrzeżenie numeru PESEL może stać się skutecznym narzędziem ochrony.

Przed zawarciem/zmianą umowy

Zgodnie z nowym art. 105d ust. 1 Prawa bankowego, banki zobowiązane będą do weryfikacji w rejestrze, czy numer PESEL konsumenta jest zastrzeżony, przed:

1) zawarciem umowy:
   a) rachunku oszczędnościowego i ROR,
   b) o wydanie instrumentu płatniczego, jeżeli przewidziano w niej możliwość zawarcia umowy kredytu lub pożyczki,
   c) kredytu,
   d) pożyczki,
   e) leasingu;
2) zmianą ww. umów, w wyniku której następuje zwiększenie zadłużenia.

Zatem od 1 czerwca 2024 r. banki będą zobowiązane do weryfikowania w rejestrze zastrzeżeń, czy PESEL konsumenta jest zastrzeżony przed zawarciem ww. umów oraz zmianą niektórych z nich, o ile będzie wiązało się to ze zwiększeniem zadłużenia. Kluczowe zatem staje się ustalenie przez banki, w jakich procesach „na ladzie" oraz zdalnych należy uwzględnić wymóg badania zastrzeżenia, obok wymogu identyfikacji i weryfikacji tożsamości klienta, przy czym istotne staje się precyzyjne określenie momentu dokonania tej weryfikacji. Ustawa odwołuje się bowiem ogólnie do chwili zawarcia umowy/jej zmiany, co w przypadku złożonych procesów bankowych, np. udzielania kredytu hipotecznego, będzie powodować wątpliwości interpretacyjne. Wydaje się, biorąc pod uwagę ratio legis ustawy, że ustawodawca posługując się zwrotem „przed zawarciem umowy" miał na myśli bezpośredni moment przed zawarciem umowy. W praktyce powinno zatem sprowadzać się to do weryfikacji zastrzeżenia na moment przed złożeniem podpisu przez ostatnią ze stron umowy. O ile w przypadku zawarcia umowy w formie elektronicznej, tj. z kwalifikowanymi podpisami elektronicznymi da się precyzyjnie określić moment zawarcia umowy, o tyle w przypadku zwykłej formy pisemnej precyzyjne określenie momentu zawarcia umowy może być utrudnione i w związku z tym nie można wykluczyć sporów w tym zakresie.

Umowy rachunku bankowego

Banki zobowiązane będą weryfikować zastrzeżenia numeru PESEL m.in. przed zawarciem umowy o prowadzenie rachunku oszczędnościowego i ROR. Wymóg ten:

1) dotyczy zarówno rachunków oszczędnościowych i ROR, prowadzonych w PLN, jak również w walutach wymienialnych,
2) nie dotyczy zawierania umów o prowadzenie rachunków terminowych lokat oszczędnościowych,

[1] Dz.U. z 2023 r., poz. 1394.

3) dotyczy co do zasady ww. umów zawieranych z konsumentem,
4) dotyczy osoby, na rzecz której ma być otwarty i prowadzony rachunek, a nie np. jej pełnomocnika.

Banki zobowiązane będą weryfikować istnienie zastrzeżenia także przed zawarciem umowy o wydanie instrumentu płatniczego, jeżeli przewidziano w niej możliwość zawarcia umowy kredytu lub pożyczki. W praktyce będą to umowy o przyznanie limitu kredytowego w karcie kredytowej.

Umowy o kredyt, pożyczkę, leasing

Głównym celem Ustawy było wprowadzenie rozwiązań zapobiegających zaciąganiu przez przestępców różnych zobowiązań – na dane identyfikujące skradzione innej osobie. Dotychczas dochodziło do wielu przestępstw, w których dane osoby postronnej były wykorzystywane przez oszustów – bez jej wiedzy i zgody – m.in. do zaciągania kredytów i pożyczek.
Zjawiskom tym ma przeciwdziałać weryfikowanie przez kredytodawcę zastrzeżenia numeru PESEL – przed zawarciem umowy kredytu, pożyczki i leasingu. Dotyczy to różnych rodzajów kredytu, ponieważ ustawodawca posługuje się ogólnym pojęciem „kredytu". Celem tego rozwiązania jest zapobieżenie (zablokowanie) zawarcia takiej umowy przez przestępcę – z wykorzystaniem numeru PESEL ofiary, która zabezpieczyła się, zastrzegając swój PESEL.
Warto także zwrócić uwagę na nowy art. 9b ustawy z 12 maja 2011 r. o kredycie konsumenckim[2]. Również on przewiduje, że kredytodawca przed zawarciem umowy o kredyt konsumencki oraz przed zmianą tej umowy, w wyniku której następuje zwiększenie zadłużenia, weryfikuje w rejestrze, czy PESEL konsumenta jest zastrzeżony.

Wyjątek

Nowy art. 9b u.k.k. przewiduje także wyjątek od obowiązku weryfikacji zastrzeżenia przed zawarciem umowy o kredyt konsumencki. I tak, zarówno obowiązku weryfikacji, jak i skutków jego niedotrzymania, nie stosuje się w przypadku, w którym łącznie spełnione będą poniższe warunki:
1) w wyniku zawarcia umowy kwota kredytu trafia nie do kredytobiorcy, lecz do sprzedawcy lub usługodawcy;
2) udzielenie kredytu następuje na odległość, z wykorzystaniem środków komunikacji elektronicznej, a kredytobiorca został uwierzytelniony;
3) kredyt udzielany jest w związku z umową o charakterze ciągłym, zawartą wcześniej przez konsumenta z danym kredytodawcą (np. w ramach przyznanego limitu do konta) oraz:
a) łączna wartość wszystkich zobowiązań do zapłaty z tytułu udzielonych kredytów w związku z ww. umową w żadnym momencie nie przekracza wysokości minimalnego wynagrodzenia za pracę[3] oraz
b) przed zawarciem ww. umowy następuje weryfikacja:
– zastrzeżenia numeru PESEL i poinformowanie konsumenta o braku weryfikacji tego zastrzeżenia przed udzielaniem poszczególnych kredytów w ramach tej umowy,
– tożsamości konsumenta.

Opisany wyjątek ma ułatwiać dokonywanie zakupów online, zwłaszcza w formule płatności odroczonych. Ustawodawca uznał, że kredyty tego rodzaju wiążą się z niższym ryzykiem i nie wymagają weryfikacji zastrzeżenia. Skutkiem wprowadzenia wyjątku od obowiązku samej weryfikacji jest również wyłączenie dla tych przypadków konsekwencji, opisanych w dalszej części, następujących w razie zawarcia umowy z konsumentem, którego PESEL był w tym czasie zastrzeżony.
O ile przepisy dotyczące weryfikacji zastrzeżenia dotyczą – co do zasady – numeru PESEL konsumenta, o tyle w jednym przypadku, tj. przy umowach o kredyt konsumencki, krąg podmiotowy został rozszerzony o osoby fizyczne, prowadzące gospodarstwo rolne. Bowiem na mocy wprowadzonego niedawno art. 2 ust. 2 u.k.k.[4], przepisy tej ustawy stosuje się również do umów o kredyt, zawieranych z osobą fizyczną prowadzącą gospodarstwo rolne.
W konsekwencji, opisany wyżej nowy art. 9b u.k.k., przewidujący obowiązek weryfikacji zastrzeżenia PESEL przez bank, będzie mieć zastosowanie również do ww. osoby fizycznej, prowadzącej gospodarstwo rolne – choć tylko w przypadku udzielania jej kredytu na podstawie tej właśnie ustawy i to – co warto podkreślić – niezależnie od celu kredytowania. Warto jednak zaznaczyć, że w ostatnim czasie rozpoczęto nowe prace legislacyjne w parlamencie, które mają na celu uchylenie ochrony konsumenckiej w stosunku do osób prowadzących gospodarstwo rolne. Ostateczny kształt przepisów w tym zakresie będzie więc zależeć od wyniku tych prac i ewentualnego uchwalenia nowych przepisów.

Weryfikacja zastrzeżenia a kredyt hipoteczny

Istotne wątpliwości budzi celowość zastosowania opisanych zasad do kredytów hipotecznych, z powodu istotnych różnic między kredytem konsumenckim a hipotecznym. Jak wiadomo, udzielenie kredytu hipotecznego poprzedzone jest kilkoma etapami, rozłożonymi w czasie (np. wniosek kredytowy, badanie zdolności kredytowej, badanie nieruchomości, decyzja kredytowa, zawarcie umowy). Powoduje to, że zaciągnięcie przez konsumenta kredytu hipotecznego trwa stosunkowo długo, co wydaje się istotnie zmniejszać ryzyko jego zaciągnięcia na skradzione dane. Wieloetapowość procesu kredytowego przy kredytach hipotecznych powoduje również, że w ich przypadku szczególnie aktualizują się wątpliwości opisywane wcześniej, a dotyczące określenia konkretnej chwili „przed zawarciem umowy", w której ma następować weryfikacja.
Co więcej, Ustawa zmienia przepisy Prawa bankowego, a w konsekwencji również u.k.k., natomiast nie zmienia ustawy o kredycie hipotecznym oraz o nadzorze nad pośrednikami kredytu hipotecznego i agentami[5], co wydaje się pewnego rodzaju niekonsekwencją po stronie ustawodawcy.

Zmiana umowy a weryfikacja zastrzeżenia

Obowiązek weryfikacji zastrzeżenia numeru PESEL aktualizuje się nie tylko przed zawarciem umowy, ale również przed zmianą umowy, o której mowa wyżej, „w wyniku której następuje zwiększenie zadłużenia". Przepis ten budzi jednak pewne wątpliwości interpretacyjne. Pojawia się pytanie, czy dotyczy to wyłącznie zmiany kwoty kredytu, czy również innych zmian umowy, które choć nie powodują zwiększenia samej kwoty kredytu, to i tak mogą powodować zwiększenie kosztów (np. przy wydłużeniu terminu spłaty kredytu).
Druga wątpliwość może dotyczyć tego, czy intencją ustawodawcy było badanie zastrzeżenia w przypadku każdej zmiany umowy kredytowej, skutkującej zwiększeniem kosztów kredytu, nawet jeśli nie wydaje się ona generować ryzyka przestępstwa z użyciem fałszywych danych (np. w przypadku zmian wynikających wprost z przepisów prawa lub dokonywanych w określo-

[2] t.j. Dz.U. z 2023 r., poz. 1028 i 1285, dalej: u.k.k.
[3] ustalanego na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę.
[4] Art. 2 ust. 2 wprowadzony przez art. 53 pkt 1 ustawy z dnia 14 kwietnia 2023 r. o konsumenckiej pożyczce lombardowej (Dz.U. z 2023 r., poz. 1285).
[5] t.j.: Dz.U. z 2024 r., poz. 2245 z późn. zm.

nych przypadkach jednostronnie przez kredytodawcę), czy jednak tylko takich zmian, które inicjowane są przez kredytobiorcę.

Przed wypłatą gotówki

Przed dokonaniem w placówce przez posiadacza rachunku, będącego konsumentem, wypłaty gotówkowej z rachunku bankowego, która pojedynczo albo jako kolejna powoduje, że suma wypłat gotówkowych w danym dniu we wszystkich placówkach danego podmiotu przekracza trzykrotność minimalnego wynagrodzenia za pracę, bank zobowiązany będzie weryfikować w rejestrze zastrzeżeń, czy PESEL posiadacza rachunku jest zastrzeżony. Jeśli tak, banki będą zobowiązane wstrzymać wypłatę na 12 godzin od momentu złożenia przez posiadacza rachunku dyspozycji wypłaty, nawet w przypadku cofnięcia w tym czasie zastrzeżenia. Wynika zatem z tego, że:

1) wymóg dotyczy wyłącznie wypłat gotówkowych z rachunku w placówce banku; nie dotyczy zatem wypłat gotówki dokonywanych np. w bankomatach czy wypłat typu cashback;
2) chodzi o wypłaty gotówkowe z rachunku danego posiadacza, będącego konsumentem; będą to zarówno wypłaty gotówkowe z ROR, z rachunków oszczędnościowych, ale również wypłaty gotówkowe będące skutkiem zapadnięcia czy likwidacji przed terminem terminowych lokat oszczędnościowych (w przypadku braku dyspozycji klienta transferu środków z lokaty na jego ROR);
3) został ustalony dzienny limit wypłat, wynoszący trzykrotność minimalnego wynagrodzenia za pracę, którego przekroczenie skutkuje po stronie banku koniecznością weryfikacji zastrzeżenia; ergo wypłaty gotówkowe do kwoty limitu nie wiążą się z koniecznością weryfikacji zastrzeżenia;
4) w przypadku istnienia zastrzeżenia banki będą zobowiązane wstrzymać wypłatę gotówkową, skutkującą przekroczeniem ww. limitu, na 12 godzin (ustanowić blokadę); nie ma tutaj znaczenia dokonanie w tym czasie cofnięcia zastrzeżenia. Po upływie czasu trwania blokady, banki będą zobowiązane zrealizować daną dyspozycję wypłaty gotówkowej (wcześniej wstrzymaną) nawet w sytuacji dalszego istnienia zastrzeżenia;
5) wymóg weryfikacji zastrzeżenia dotyczy posiadacza rachunku, a nie np. ustanowionego przez niego pełnomocnika.

RYZYKA DLA BANKÓW

Nowe przepisy przewidują rygorystyczne konsekwencje zawarcia umowy z konsumentem, którego PESEL był zastrzeżony w chwili jej zawarcia. Co ciekawe, przepisy nie zawierają wprost zakazu zawarcia umowy w przypadku istnienia zastrzeżenia. Przewidują jednak, że jeśli w chwili zawarcia umowy PESEL konsumenta był zastrzeżony (tj. albo nie dokonano weryfikacji, albo zawarto umowę mimo zastrzeżenia, albo dokonano weryfikacji na zbyt wczesnym etapie i klient dokonał późniejszego zastrzeżenia jeszcze przed zawarciem umowy) – banki nie będą mogły domagać się od konsumenta zaspokojenia roszczenia z tytułu zawarcia tej umowy ani też zbyć powstałej z niej wierzytelności. Skutek ten rozciąga się również na następców prawnych konsumenta.

Nieprecyzyjność przepisów może być też okazją do nadużyć, zmierzających do zaciągnięcia zobowiązania i uchylenia się od jego realizacji, z powołaniem na brak możliwości dochodzenia przez bank roszczeń z tytułu danej umowy, właśnie z uwagi na zastrzeżenie numeru PESEL. Sytuacja taka może wystąpić zwłaszcza w przypadku dokonania zastrzeżenia w ostatnim momencie, tuż przed zawarciem umowy (a niekiedy może to być kwestia nawet kilku minut lub sekund).

Uwagę zwraca również pewna niekonsekwencja w określeniach ustawowych. Z jednej bowiem strony w przepisie mowa jest o weryfikacji zastrzeżenia „przed zawarciem umowy”, z drugiej natomiast – w kontekście konsekwencji zawarcia umowy mimo zastrzeżenia – mowa jest o sytuacji, w której okaże się, że „w chwili zawarcia umowy” PESEL konsumenta był zastrzeżony. Tymczasem w znaczeniu stricte prawnym określenia te nie są tożsame, co w praktyce może powodować kolejne wątpliwości interpretacyjne.

Z tych względów szczególnie istotne jest, by – tak jak wskazywano wcześniej – weryfikacja dokonywana była w momencie bezpośrednio przed zawarciem umowy, tj. „jak najbliżej” chwili, w której następuje formalny skutek zawarcia umowy.

ASPEKTY BIZNESOWE I TECHNICZNE

Rejestr zastrzeżeń numerów PESEL jest udostępniany i administrowany przez Ministerstwo Cyfryzacji. Dostęp do niego banki mogą otrzymać bezpośrednio przez Ministerstwo Cyfryzacji lub za pośrednictwem ZBP i należącego do niego Systemu Dokumenty Zastrzeżone.

W obu wariantach każdy z banków będzie musiał przejść ścieżkę dostępową, która zaczyna się od przeprowadzenia prac technicznych, następnie złożyć formalny wniosek do Ministra Cyfryzacji oraz otrzymać pozytywny wynik przeprowadzonego audytu. Na koniec wydawana jest decyzja, na podstawie której bank będzie mógł łączyć się z rejestrem.

Od strony technicznej mogą wystąpić planowane oraz nieplanowane przerwy w dostępie do rejestru. W przypadku niedostępności planowanej odpowiedzialność banku nie ustaje, tzn. bank musi dokonać wyboru, czy zawrze umowę z klientem lub wypłaci gotówkę, przekraczającą opisany wyżej limit – nie odpytując rejestru.

Natomiast jeśli przerwa w dostępie do rejestru nie była planowana, wówczas – po ponownej nieudanej próbie weryfikacji – bank może:

1) odmówić zawarcia umowy
2) zawrzeć umowę, pod warunkiem spełnienia określonych wymogów – wówczas odpowiedzialność banku może ustać, jeśli:
   - dokonano ponownej nieudanej próby weryfikacji zastrzeżenia po upływie 15 minut od pierwszej weryfikacji,
   - zachowano należytą staranność przy weryfikacji tożsamości konsumenta i udokumentowano dokonanie weryfikacji.

Niedostępności systemu, które są planowane, zwykle realizowane są w późnych godzinach nocnych, aby miały jak najmniejszy wpływ na działalność operacyjną różnych instytucji. Informacje o planowanych godzinach niedostępności będą z wyprzedzeniem publikowane w BIP.

WNIOSKI

Wprowadzenie narzędzia, jakim jest zastrzeżenie numeru PESEL – w świetle jego konstrukcji i łatwości jego dokonania – wydaje się być dobrym kierunkiem legislacyjnym i krokiem zmierzającym do zwiększenia ochrony osób fizycznych przed skutkami przestępstw, takich jak kradzież tożsamości czy wyłudzenia metodą „na wnuczka”.

W praktyce natomiast skuteczność tego narzędzia będzie zależała od kilku czynników, w szczególności od upowszechnienia dokonywania zastrzeżeń wśród społeczeństwa. Natomiast po stronie instytucji zobowiązanych kluczowe wydaje się nie tylko dostosowanie regulacji, procesów i wykorzystywanych systemów informatycznych, ale także położenie szczególnego nacisku na szkolenia personelu, mającego bezpośredni kontakt z klientem. Tak naprawdę to na personelu będzie bowiem ciążył obowiązek dopełnienia obowiązków ustawowych, związanych z weryfikacją istnienia zastrzeżenia w przypadkach wymaganych prawem. Znaczenie będą miały również aspekty czysto techniczne, związane z funkcjonowaniem rejestru zastrzeżeń, takie jak np. ewentualna niedostępność rejestru, spowodowana awarią. ●

OFERTA SZKOLENIOWA

KWIECIEŃ - CZERWIEC 2024

ZAPRASZAMY DO UDZIAŁU W NASZYCH AKADEMIACH:

- Profesjonalny pracownik bankowy
- Monitoringu Kredytowego
- Compliance
- Kredytowa
- Lidera
- Egzekucji z Rachunku Bankowego

ROZWIJAJ Z NAMI SWOJE KOMPETENCJE!

Zapraszamy do współpracy i do kontaktu:

sesje@bodie.pl

BODiE
Grupa SGB