BANK SPÓŁDZIELCZY

10 lat iPS SGB

ŚWIAT BANKOWOŚCI SPÓŁDZIELCZEJ
NR 4/618 PAŹDZIERNIK – GRUDZIEŃ 2025
ISSN 2719-4515

Zespół to nasza energia

rozmowa z Anną Kozłowską

s. 5

Cyberbezpieczeństwo

s. 10-42

ROK STRATEGICZNYCH DECYZJI

Zwykle końcówka roku skłania nas do podsumowań, analiz i wyciągania wniosków. To naturalny moment, w którym spoglądamy wstecz, by z dystansu ocenić, jakie plany udało się zrealizować i w jakim kierunku powinniśmy podążać dalej. A mijający rok naprawdę dał nam wiele materiału do refleksji, bo w Spółdzielczej Grupie Bankowej działo się więcej niż zwykle.

Był to rok decyzji o strategicznym znaczeniu i momentów, które będą kształtować naszą przyszłość przez kolejne lata. W kwietniu, podczas Zgromadzenia Prezesów w Kołobrzegu, przyjęto nową strategię z hasłem „Więcej niż biznes". To nie tylko dokument, to deklaracja ambicji i przekonania, że bankowość spółdzielcza jest czymś znacznie większym niż zestaw produktów i usług. Jest przestrzenią odpowiedzialności, współpracy i budowania lokalnej siły.

Kilka tygodni później wybrano nową Radę Nadzorczą SGB-Banku, co otworzyło kolejny etap w kształtowaniu kierunków rozwoju. A jesienią, gdy liście zaczęły opadać z drzew, tempo zmian ani na moment nie zwolniło – prezesi powołali nową Radę Zrzeszenia SGB. To symboliczne domknięcie cyklu zmian personalnych i organizacyjnych, które w tym roku wyznaczyły nowe ramy funkcjonowania SGB.

Rok 2025 był również czasem intensywnej komunikacji marketingowej. Postawiliśmy na nią mocno po przyjęciu nowej strategii. Kampanie od wiosennych „Młodych Wilków", przez kredyty hipoteczne, aż po ofertę dla przedsiębiorców - spotkały się z dobrym odbiorem i odpowiadały na realne oczekiwania klientów.

Podobną uwagę do obecności w lokalnej świadomości przykładają też banki spółdzielcze, jak choćby Bank Spółdzielczy w Lipnie, który w tym roku świętował jubileusz, obok 50 innych banków reprezentujących SGB. O naszych nowych produktach, wsparciu marketingowym i sile lokalności mówi też Anna Kozłowska, prezes tego banku: „Zespół to nasza energia'' – to mocny głos o przyszłości i ludziach, którzy tę przyszłość budują.

W tym numerze wracamy również do wydarzenia epokowego czyli powstania IPS-SGB. To rozwiązanie było w Polsce pionierskie: uruchomić system stworzony przez banki spółdzielcze, by wspólnie dbać o bezpieczeństwo, nadzór ryzyka i stabilność całego Zrzeszenia.

Warto wrócić zarówno do samego okresu, jak i wspomnień osób, które ten system tworzyły. Początki IPS-SGB wspominają nie tylko osoby będące wówczas w kadrze zarządzającej, ale również pierwsi pracownicy, którzy zostali tam zatrudnieni. Bez zaangażowania każdego z nich nie byłoby spółdzielczego systemu ochrony, jaki dzisiaj znamy.

Polecam także rozmowę z Michałem Ołdakowskim, prezesem zarządu IPS-SGB: „Cała umowa Systemu Ochrony SGB, mająca charakter wielostronny, jest potwierdzeniem solidarności banków Spółdzielczej Grupy Bankowej. Ta wspólnota bezpieczeństwa jest siłą, której banki komercyjne nie mają" – mówi prezes Ołdakowski.

Drugim przewodnim tematem numeru jest cyberbezpieczeństwo. Dziś żyjemy równocześnie w dwóch światach – rzeczywistym i cyfrowym. Kupujemy więcej online, w smartfonie trzymamy niemal całe nasze życie, płacimy telefonem lub zegarkiem. Przestępcy doskonale wykorzystują naszą nieuwagę, roztargnienie i emocje. Dlatego tak wiele materiałów w tym numerze to praktyczne wskazówki, jak nie dać się oszukać. Cieszy nas, że swoją wiedzą i doświadczeniem dzielą się pracownicy SGB-Banku, którzy na co dzień pracują w obszarze cyberbezpieczeństwa. Doskonale wiemy, że cyberbezpieczeństwo, to gra zespołowa.

Grupa SGB dokłada wszelkich starań, aby środki naszych klientów były bezpieczne. W rozmowie z nami Krzysztof Dąbrowski, dyrektor zarządzający Pionem Bezpieczeństwa UKNF, podkreśla: „Centralizacja procesów cyberbezpieczeństwa oraz budowanie spójnych procedur, a nawet struktur takich jak SOC, jest właściwym kierunkiem, który realnie zwiększa cyberodporność członków Grupy".

Co jeszcze w naszym magazynie? Między innymi o tym, jak budujemy galaktykę nowych możliwości. Każdy projekt edukacyjny, to jak kolejna jaśniejsza gwiazda na mapie kompetencji — gwiazda, która pomaga naszym pracownikom odnajdywać się w dynamicznym świecie finansów. Polecam tekst Grażyny Koziołek.

Jak zwykle znajdziecie także recenzje, raporty i porady prawne. Na koniec polecam rozmowę z Jackiem Walkiewiczem. Jego przesłanie jest wyjątkowo aktualne: „Niezależnie od tego, co się dzieje, najlepszym lekarstwem na zmartwienia jest drugi człowiek. Dbajmy o relacje z bliskimi, dziećmi, rodzicami, klientami, przyjaciółmi i z ludźmi, których spotykamy na ulicy".

Dołączam się do tych słów. W imieniu całej redakcji życzę Państwu w nadchodzącym 2026 roku dużo życzliwości, zdrowia, uśmiechu i serdeczności. Dbajmy o siebie nawzajem. Dbajmy o relacje.

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**
M.: +48 692 465 136, e-mail: roman.szewczyk@sgb.pl
Redaktorzy prowadzący – **Rafał Łopka, Jerzy Sygidus**
Korekta: **Jerzy Sygidus**
Projekt i skład: **dubielstudio.pl, Marek Kozakowski**
Stale współpracują: **Robert Azembski, Andrzej Borowiak, Janusz Orłowski, Agnieszka Szelejewska, Krzysztof Swoboda**

Zdjęcie na okładce: **Roman Szewczyk**
Obróbka: **dubielstudio.pl**
Zdjęcia we wnętrzu pochodzą z **Pixabay.com**, **Unsplash.com i shutterstock.com**.

BS
NA RYNKU OD
1964 ROKU

Wydawca:
Bankowy Ośrodek Doradztwa i Edukacji Sp. z o.o.
Szarych Szeregów 23a, 60-462 Poznań,
Na zlecenie SGB-Banku.

BS

SPIS TREŚCI

KLIKNIJ ŻEBY PRZEJŚĆ DO ARTYKUŁU

BS

SPIS TREŚCI

KLIKNIJ ŻEBY PRZEJŚĆ DO ARTYKUŁU

ROZMOWA NUMERU

Zespół to nasza energia

Rozmowa z **Anną Kozłowską**,
prezes Zarządu Banku Spółdzielczego w Lipnie

FOT. ROMAN SZEWCZYK

Kredyt jubileuszowy na 9,59% w skali roku, gdy konkurencja oferuje 12% i więcej... Czy to jest sposób na przyciągnięcie nowych klientów? Walka o lokalny rynek? Element długoterminowej strategii? Jak traktować taką ofertę?

W ofercie naszego banku zawsze posiadamy produkt z atrakcyjną ceną dla obecnych i nowych klientów. W portfelu kredytowym osoby prywatne posiadają 68 mln złotych kredytów konsumpcyjnych, co stanowi 28% struktury. Naszą działalność prowadzimy głównie na terenie powiatu lipnowskiego, w tym w mieście Lipno, w którym zamieszkuje ok. 14 tys. mieszkańców. Dostępność placówek i wykwalifikowana kadra pracowników to atuty, które przyciągają nowych klientów, a jeśli do tego produkt ma dobrą cenę, o nowych klientów jest łatwiej. Nieodłącznym elementem naszej aktywności jest także reklama w mediach (radio regionalne, kino miejskie, telewizja lokalna), a obecnie istnieje możliwość przedstawiania oferty również

z wykorzystaniem kanałów elektronicznych np. dzięki bankowości mobilnej.
Strategia banku zawsze ukierunkowana jest na udoskonalanie oferty i posiadanie gamy produktów dla klientów z różnych segmentów i branż. W zakresie chęci skorzystania z kredytu gotówkowego, bo o takim tu mowa, zauważamy dwa kierunki. Pierwszy dotyczy potrzeby szybkiego dostępu do finansowania z pełnym wykorzystaniem technologii i bez wychodzenia z domu. To ma być krótki proces, nawet taki, który zamyka się w minutach, na bieżące lub spontaniczne potrzeby.

Nieodłącznym elementem naszej aktywności jest także reklama w mediach (radio regionalne, kino miejskie, telewizja lokalna).

Jest też drugi kierunek – może trochę dłuższy, związany z potrzebą obecności w oddziale czy placówce banku, w której klient słabiej zorientowany technologicznie, po rozmowie z pracownikiem banku i dopasowaniu produktu do jego potrzeb, szybko może uzyskać finansowanie. Mam na myśli proces realizowany z wykorzystaniem Platformy SGB, w której możemy stosować uproszczony proces scoringowy.

Klienci to doceniają?

Tak. Nasi klienci wysoko cenią doradztwo i dopasowanie produktu do ich potrzeb i możliwości, co bezpośrednio przekłada się na dobrą jakość naszego portfela kredytowego. Warto wskazać, że aby zwiększyć udział w rynku kredytów gotówkowych proces kredytowy dla osób fizycznych winien być skrócony do minimum, w oparciu o model scoringowy i w krótkim czasie. Jeżeli takie narzędzia banki spółdzielcze będą mogły wdrożyć, zyskają możliwość zwiększania udziału w rynku.
Wprowadziliśmy do oferty kredyt online. Klienci bardzo na niego czekali. Rynek, mimo wyższego kosztu kredytu dla klientów indywidualnych, wygrywa krótkim procesem. Mam nadzieję, że za 12 miesięcy z poczuciem dobrze wykonanej pracy i dzięki wykorzystaniu rozwiązań technologicznych, udział kredytów gotówkowych w portfelu kredytowym naszego banku będzie wyższy.

Siłą banków spółdzielczych jest ich lokalny charakter i bliskość z klientem. Co jest siłą Banku Spółdzielczego w Lipnie.

– Do tej bliskości i lokalnego charakteru dołączyłabym stwierdzenie, że siłą każdej firmy są ludzie, którzy od pokoleń każdego dnia podejmują decyzje, rozpatrują inicjatywy, budują instytucję silną kapitałem ludzkim, majątkiem rzeczowym i funduszami własnymi. Te wszystkie elementy pozwalają dumnie podkreślić, że Bank Spółdzielczy w Lipnie to silna kapitałowo instytucja. Możliwości finansowania mamy bardzo wysokie, maksymalne zaangażowanie w jeden podmiot i podmioty powiązane przy 25% kapitałów banku to wartość ok. 19 mln. złotych. A zatem nasz bank może finansować całkiem duże projekty.

A pracownicy?

– Głównym atutem naszego banku jest wykwalifikowana, ciągle rozwijająca się kadra pracowników, bardzo otwarta na nowe pomysły i cele do realizacji. Średnia wieku pracowników banku wynosi 41 lat, a stażu pracy 19 lat, więc pragnę jednoznacznie potwierdzić, że z nowymi technologiami nie mają żadnego problemu i z otwartością promują i wspierają klientów w korzystaniu z tych rozwiązań. Zatrudniamy 68 osób. Poza wynagrodzeniem, konkurencyjnym na lokalnym rynku, oferujemy szereg benefitów im. premie dwa razy w roku, spotkania integracyjne itp.

Na stronie internetowej banku można zauważyć wyraźny podział oferty skierowanej do różnych grup klientów m.in. do przedsiębiorców. Właśnie jesteśmy na półmetku kampanii reklamowej „Dla firm. Dla Każdego”. Jak pani ocenia kampanię? To już trzecia kampania reklamowa SGB w tym roku.

Tak jak pan zauważył, Bank Spółdzielczy w Lipnie posiada ofertę produktową dla wielu grup klientów, branż i sektorów gospodarki. Każda kampania, którą na przestrzeni ostatnich lat kierujemy do różnych grup klientów, w mojej ocenie jest profesjonalnie przygotowana i bardzo dobrze, że to już kolejna w tym roku.
Zarówno kampania dla młodych, kampania kredytu hipotecznego oraz obecna świetnie wpisują się w DNA Banków Spółdzielczych SGB i skierowane są do klientów, na których nam bardzo zależy. Być może dzięki nim każdy mieszkaniec naszego kraju zauważy, że banki spółdzielcze tworzące Grupę SGB, są bankami uniwersalnymi i mają ofertę dla każdego. Podkreślam też przy okazji, że do promocji spotów reklamowych wykorzystujemy nasze lokalne media – one są najbliżej klientów i cieszą się ich dużym zaufaniem. To także ułatwia odbiór naszych kampanii.

Głównym atutem naszego banku jest wykwalifikowana, ciągle rozwijająca się kadra pracowników, bardzo otwarta na nowe pomysły i cele do realizacji.

Od 2021 roku Bank Spółdzielczy w Lipnie korzysta z Systemu Usług Zrzeszeniowych (SUS). Jakie konkretne korzyści przyniosło wdrożenie systemu klientom i samemu bankowi.

W jednym zdaniu można by wskazać, że to bezpieczeństwo funkcjonowania oraz możliwość oferowania usług i produktów w nowoczesnej i bezpiecznej technologii. Korzystanie z rozwiązania SUS pozwala bankowi optymalizować procesy operacyjne, a to ma znaczenie, gdyż bank nie zwiększa udziału pracowników w sferze back office i realizuje coraz więcej zadań i obowiązków raportowych i analitycznych. Tym samym pozwala to zwiększać skalę działalności przy wykorzystaniu takiego samego zespołu pracowników.
Nie ulega wątpliwości, że uruchamiane rozwiązania i systemy – mam tu na myśli Platformę SGB, Moje dokumenty SGB, logowanie kodem QR i kredyt online, bankowość internetową z nowymi funkcjonalnościami i oczywiście bankowość mobilną – wspierają i wnoszą wartość dodaną w postaci optymalizacji procesów i dysponowania rozwiązaniami takimi, jakie posiadają banki komercyjne. Nie możemy nie wspomnieć o usłudze BLIK i BLIK Płacę później, karcie wielowalutowej, Kantorze SGB, koncie dla młodych. Można jednoznacznie stwierdzić, że obecna oferta dostępna z poziomu telefonu, jest bardzo bogata. Gdzie byśmy byli bez tych rozwiązań dostarczanych przez bank zrzeszający?
Pragnę wyrazić swoją opinię i stwierdzić, że jesteśmy zrzeszeniem pierwszej prędkości. Liczba projektów i inicjatyw re-

Centrala banku przy ulicy Włocławskiej.
To nowoczesna przestrzeń dla klientów i pracowników.

alizowana w każdym roku jest imponująca. Każdy z banków spółdzielczych może wybrać sobie usługi i funkcjonalności, z których chce korzystać.
Cenne jest również to, że usługi i produkty ze sfery bezpieczeństwa udostępniane są również bankom, które nie korzystają z rozwiązania zrzeszeniowego. Na jeszcze jeden element warto zwrócić uwagę przy rozpatrywaniu rozwiązania zrzeszeniowego – na budowanie funduszu rozwojowego, dzięki któremu zostały sfinansowane różne inicjatywy zarówno produktowe, jak i w sferze bezpieczeństwa.

Liczba projektów i inicjatyw realizowana w każdym roku jest imponująca. Każdy z banków spółdzielczych może wybrać sobie usługi i funkcjonalności, z których chce korzystać.

To są argumenty, które potwierdzają, że do banku spółdzielczego trafi klient młody albo taki, który zdecyduje się na zmianę banku, bo przecież przyświeca nam idea „Mamy tu wszystko”. Pragnę też zauważyć, że to samo się nie zadzieje, potrzebna jest aktywna praca naszych pracowników, którzy bardzo często wypełniają rolę doradców, a także aktywna reklama i kampanie promujące SGB. Moim zdaniem, w tym obszarze jest jeszcze sporo do zrobienia. Wdrażanie rozwiązań optymalizujących czynności i procesy w celu doskonalenia jakości obsługi klienta to nasz cel przyjęty w strategii banku na lata 2025-2028.

Cyberbezpieczeństwo staje się jednym z najważniejszych obszarów działalności banków. Jak Bank Spółdzielczy w Lipnie dba o bezpieczeństwo danych i środków swoich klientów? Czy podejmujecie Państwo działania edukacyjne, na przykład szkolenia czy kampanie ostrzegające przez oszustami internetowymi.

O bezpieczeństwo danych i środków naszych klientów dbamy na wielu płaszczyznach. Doceniamy i włączamy się we wszystkie rozwiązania oferowane w ramach SUS, dbamy o modernizację i bezpieczeństwo infrastruktury IT banku. Organizujemy też spotkania z klientami banku, podczas których jednym z tematów jest bezpieczeństwo danych po stronie klientów, osób prywatnych, właścicieli film, urzędników. Szkolimy pracowników i uczulamy starszych klientów, którzy często nadal odwiedzają nasze placówki. W ramach działań edukacyjnych, które prowadzimy w szkołach w projekcie „BAKCYL” Warszawskiego Instytutu Bankowości, oraz spotkaniach w banku, bezpieczeństwo w sieci jest również ważnym tematem.

W ostatnich latach coraz więcej klientów korzysta z bankowości mobilnej i internetowej. Jakie rozwiązania w tym zakresie oferuje bank i w jaki sposób zapewnia bezpieczeństwo?

Bankowość internetową uruchomiliśmy w 2003 roku dla jednostki samorządu terytorialnego. Korzystaliśmy wówczas ze współpracy z innym dostawcą usługi. Sukcesywnie od wielu lat udostępnialiśmy naszym klientom tę formę korzystania z dostępu do rachunku bankowego. Obecnie z bankowości internetowej korzysta 7758 klientów banku, w tym 3120 w sposób aktywny. Z aplikacji SGB Mobile korzysta 6441 klientów, w tym aktywnych jest 5243 klientów. Jest to dobry wskaźnik, ale uważam, że jeszcze mamy sporo do zagospodarowania. Cieszy nas fakt posiadania bankowości mobilnej, wciąż rozwijanej o nowe funkcjonalności, z których klienci bardzo chętnie korzystają. To również pozwala zdobywać młodych klientów.

Kampania dla młodych, promocja kredytu hipotecznego oraz obecna kampania adresowana do przedsiębiorców, świetnie wpisują się w DNA Banków Spółdzielczych SGB i skierowane są do klientów, na których nam bardzo zależy. Być może dzięki nim każdy mieszkaniec naszego kraju zauważy, że banki spółdzielcze tworzące Grupę SGB są bankami uniwersalnymi i mają ofertę dla każdego.

Czy w planach banku są inwestycje w nowe technologie – takie jak sztuczna inteligencja, ▶

automatyzacja procesów czy analityka danych – które mogą nie tylko usprawnić obsługę klientów, ale też zwiększyć poziom bezpieczeństwa?

Bez wahania mogę to potwierdzić. A szerzej, ja osobiście oczekuję i na bieżąco śledzę planowane projekty w ramach SUS. Zarządu Banku Spółdzielczego w Lipnie nie trzeba przekonywać do nowych technologii. Bardzo nam zależy na posiadaniu rozwiązań zarówno front office, jak również zwiększających bezpieczeństwo. Potwierdzeniem moich słów jest fakt udziału pracowników banku w pilotażach projektów informatycznych realizowanych przez bank zrzeszający. Od nowych technologii nie ma odwrotu, zakres sprawozdawczy i raportowy bez udziału technologii nie będzie mógł być zrealizowany. Oczekujemy na uruchomienie kolejnych rozwiązań np. cyfrowe repozytorium, podpis cyfrowy, cyfrowy obieg dokumentów, multibiznes w kontekście optymalizacji procesów ale i obniżenia kosztów działalności.

Korzystanie z rozwiązania SUS powala bankowi optymalizować procesy operacyjne, a to ma znaczenie, gdyż bank nie zwiększa udziału pracowników w sferze back office i realizuje coraz więcej zadań i obowiązków raportowych i analitycznych.

Bank Spółdzielczy w Lipnie obchodzi w tym roku 80 lat działalności. Czy z okazji jubileuszu przygotowujecie specjalne wydarzenie lub ofertę dla swoich klientów?

Tak to prawda, w sierpniu 2025 r. minęła 8 dekada działalności banku. Osiemdziesiąt lat działalności Banku Spółdzielczego w Lipnie to wiele zapisanych kart i dokumentów o historycznym znaczeniu. Jednakże bohaterami bogatej historii banku obok wydarzeń i faktów, są przede wszystkim ludzie, dla których siła i potencjał tej instytucji zawsze były najwyższym dobrem.
Dbając o potencjał ekonomiczny w misję działalności banku zawsze wpisują się działania społeczne. Jesteśmy czynnym uczestnikiem inicjatyw kulturalnych, charytatywnych i sportowych oraz edukacyjnych.
Jak zaakcentowaliśmy ten jubileusz? Po pierwsze przeznaczyliśmy część wypracowanego wyniku finansowego z 2024 r. na zasilenie funduszu udziałowego, funduszu naszych członków, (właścicieli banku), których na 31.12.2024 r. było 1964, i posiadających 2951 jednostek udziałowych poprzez przekazanie każdemu członkowi banku, zgodnie z uchwałą zebrania przedstawicieli, dodatkowej jednostki udziałowej w kwocie 650,00 zł. co dało łączną kwotę 1.577.092,00 zł., Ta decyzja została bardzo dobrze przyjęte przez delegatów czyli przedstawicieli członków banku. Ważnym elementem zasilenia jest fakt możliwości pobrania tej dodatkowej jednostki bez utraty prawa członkostwa.
Pragnę dodać, że w historii banku tak wysoka „dywidenda" nie była nigdy przekazana udziałowcom. Zawsze priorytetem było budowanie funduszu zasobowego dającego siłę kapitałową. Nasze działania w roku jubileuszowym obejmowały również inne atrakcje dla członków, klientów i pracowników oraz emerytowanych pracowników m.in. wyjazdy na koncerty, wystawy i spotkanie integracyjne. Dodatkowo dla pracowników Zarząd banku przeznaczył gratyfikację pieniężną proporcjonalną do lat pracy w banku.

Za nami rok 2025 – z malejącą inflacją, niepewnością gospodarczą, ale też ze stabilizacją sektora finansowego. Czy to był dobry rok dla Banku Spółdzielczego w Lipnie?

Bardzo dobry. Kolejny rok zakończy się bardzo dobrym wynikiem finansowym, z niskim poziomem ryzyka, dobrą jakością portfela kredytowego, bardzo dobrą adekwatnością kapitałową, z przyrostem kart płatniczych, kredytów, a przede wszystkim z uruchomionymi nowymi usługami dla naszych klientów. Podobnie jak w całym sektorze, nadpłynność finansowa banku powoduje, że zależy nam na zwiększeniu akcji kredytowej. Czynniki otoczenia makroekonomicznego oraz wysokie stopy procentowe bardzo mocno wyhamowały inwestycje zarówno w sektorze Agro jak i MŚP. Dla sektora finansowego, ale nie tylko, także dla całej gospodarki, ważna jest równowaga gospodarcza. Niepewności związane z minionym czasem szczęśliwie są już za nami, cenny jest fakt unormowania inflacji, a więc wrócił optymizm i inwestycje. My nadal będziemy robić swoje, unowocześniać procesy, przedstawiać bank jako uniwersalny, pozyskiwać klientów od konkurencji oraz rozwijać kompetencje pracowników.

Czego życzyłaby pani klientom i pracownikom banku z okazji jubileuszu?

Podczas podsumowania każdego roku działalności naszego banku składam serdeczne podziękowania udziałowcom banku, a za ich pośrednictwem wszystkim klientom banku, przede wszystkim za mądrość w podejmowaniu decyzji strategicznych. Życzę, żeby wszystkim po prostu dobrze się powodziło, żeby pasmo sukcesów zawodowych i osobistych prowadziło do realizacji przewagi konkurencyjnej, co stanie się sukcesją dla następnych pokoleń.
Pracownikom zawsze dziękuję za ogromne zaangażowanie, za wysoką etykę pracy, za otwartość na nowe wyzwania. Dziękuję też za to, że wykonują codzienne swoje czynności z ogromną odpowiedzialnością, za co na moje ręce przekazywane są podziękowania i uznania. To właśnie pracownicy, każdego dnia „małą łyżeczką" powiększają potencjał i bezpieczeństwo instytucji finansowej.
Wszystkim klientom, członkom, przyjaciołom banku, szczególnie obecnym i emerytowanym pracownikom banku, składam serdeczne podziękowania za zaufanie i wzajemnie korzystną współpracę, życzę zdrowia i wszelkiej pomyślności w życiu prywatnym. Niech kolejne lata będą również udane i pełne sukcesów.

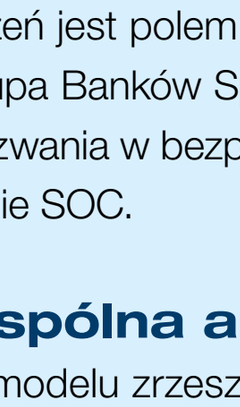
Można jednoznacznie stwierdzić, że obecna oferta dostępna z poziomu telefonu, jest bardzo bogata. Gdzie byśmy byli bez tych rozwiązań dostarczanych przez bank zrzeszający?

Rozmawiał: Roman Szewczyk
Lipno, 15 grudnia 2025 r.

Bank Spółdzielczy SGB dla firm

SGB Bank Spółdzielczy | Dla firm. Dla każdego!

SOC SGB – fundament bezpieczeństwa banków spółdzielczych



Daniel Krzywiec
SGB-Bank

SOC SGB to wizytówka strategicznej decyzji prezesów banków spółdzielczych, która uczyniła grupę SGB jednym z najbardziej zaawansowanych technologicznie i operacyjnie centrum cyberbezpieczeństwa w polskiej bankowości. To fundamentalna decyzja, która gwarantuje bezpieczeństwo i stabilność wszystkim bankom Spółdzielczym SGB.

„W świecie, w którym banki i ich klienci są codziennie atakowani, a cyberprzestrzeń jest polem bitwy, kluczem do przetrwania i rozwoju jest zjednoczenie sił. Grupa Banków Spółdzielczych SGB udowodniła, że potrafi przekuć największe wyzwania w bezprecedensową przewagę, stawiając na skonsolidowane rozwiązanie SOC.

Wspólna architektura chmurowa

W modelu zrzeszeniowym wdrożyliśmy jedną wspólną platformę cyberbezpieczeństwa dla wszystkich Banków Spółdzielczych SGB. Zamiast setek różnorodnych systemów, banki spółdzielcze działają na wspólnym, standaryzowanym stosie technologicznym. Takie podejście przynosi szereg kluczowych korzyści, które transformują bankowość spółdzielczą, czyniąc ją bardziej bezpieczną, efektywną i konkurencyjną. Korzystanie z jednej wspólnej, centralnej infrastruktury chmurowej zastępuje konieczność indywidualnych inwestycji w serwery i oprogramowanie w każdym z banków spółdzielczych. Ekonomia skali jest kluczowym uzasadnieniem dla konsolidacji i centralizacji usług SOC w grupie SGB. Dzięki temu każdy bank spółdzielczy ma dostęp do rozwiązań klasy enterprise (przeznaczonych dla najwięk-

szych instytucji), które samodzielnie trudno byłoby sfinansować. Z perspektywy banków spółdzielczych wysokie koszty inwestycyjne zastąpiły dużo mniejsze przewidywalne koszty operacyjne. Zespoły IT w bankach spółdzielczych nie są obciążone skomplikowanym zarządzaniem systemami bezpieczeństwa i infrastrukturą chmurową. Mogą skupić się na wspieraniu lokalnego biznesu, relacjach z klientami i wdrażaniu gotowych rozwiązań dostarczanych centralnie.
„SOC SGB to zaawansowana, wielowarstwowa platforma cyberbezpieczeństwa,

Najważniejszą korzyścią jest możliwość skonsolidowania kompetencji eksperckich w jednym miejscu.

która dzięki architekturze chmurowej i wykorzystaniu AI, gwarantuje najwyższy poziom bezpieczeństwa ICT oraz ochronę klientów, obejmując centralnie całe zrzeszenie Banków Spółdzielczych SGB. Banki spółdzielcze, odciążone od kompleksowego zarządzania cyberbezpieczeństwem, mogą skupić swoje zasoby i czas na relacjach z klientami, doradztwie i sprzedaży."

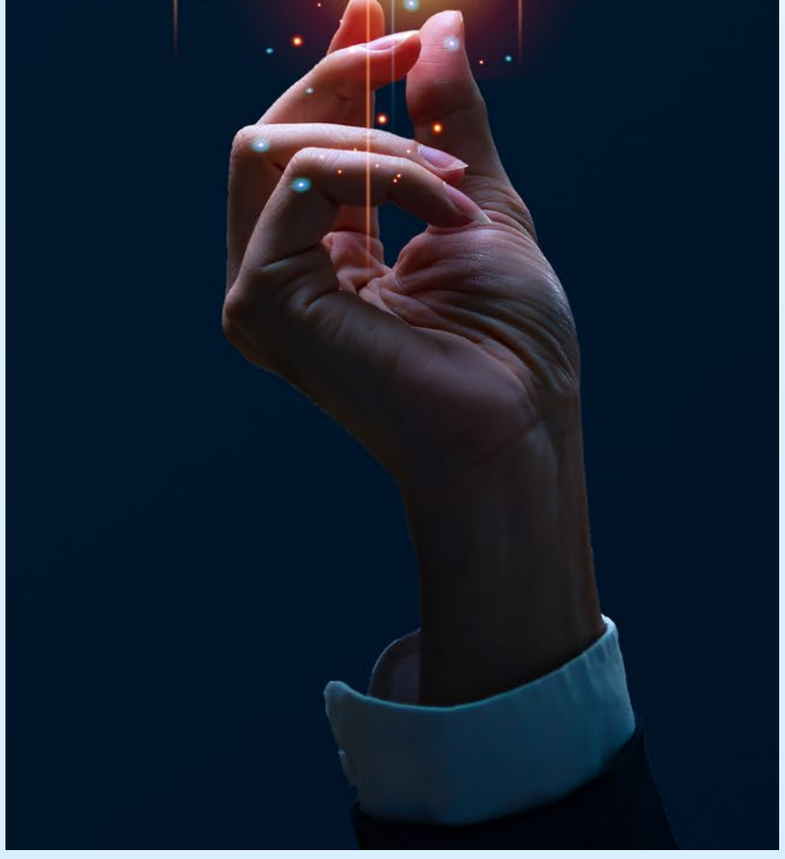
Optymalizacja zasobów personalnych

SOC SGB to przede wszystkim maksymalizacja dostępności i jakości specjalistycznych kompetencji, przy jednoczesnej redukcji kosztów dla pojedynczego banku spółdzielczego. Banki spółdzielcze, często zlokalizowane w mniejszych miejscowościach, mają utrudniony dostęp do wysoko wykwalifikowanych specjalistów. Dzięki centralizacji, uzyskują dostęp do jednego wspólnego zespołu SOC, bez potrzeby zatrudniania i utrzymywania ekspertów cyberbezpieczeństwa, chmury i zaawansowanej analityki. Finalnie, koszt utrzymania wysoce wyspecjalizowanego zespołu SOC jest rozłożony na całą Grupę, co jest wielokrotnie tańsze dla każdego banku niż samodzielne budowanie takiej jednostki. Centralizacja chroni banki spółdzielcze przed paraliżem operacyjnym, np. w przypadku odejścia kluczowego specjalisty. W grupie SGB stawiamy na standaryzację i rozwój kadr SOC w modelu centralnym, co sprzyja tworzeniu ujednoliconych ścieżek rozwoju i szkoleń. Wdrażamy ujednolicone programy szkoleniowe i procedury operacyjne, co zapewnia jednolity, wysoki poziom wiedzy i minimalizuje ryzyko błędu ludzkiego. Centralny SOC pełni rolę edukacyjną, podnosząc świadomość na temat zagrożeń i promując kulturę bezpieczeństwa wśród wszystkich pracowników zrzeszenia.

SOC SGB to zespół ekspertów

(analityków i inżynierów bezpieczeństwa), których wiedza jest wspólna dla wszystkich uczestników usługi SOC. Wdrożony model umożliwia wspólne zarządzanie wiedzą, gdzie wszelkie incydenty, najlepsze praktyki i procedury opracowane przez centralny zespół natychmiast zasilają wiedzą całe zrzeszenie. Oznacza to szybką, skoordynowaną i profesjonalną reakcję, która minimalizuje straty wizerunkowe i finansowe. SOC SGB widzi wspólny horyzont zagrożeń, monitoruje i analizuje incydenty bezpieczeństwa dla banków spółdzielczych, zapewniając jednolitą ochronę i szybkie reagowanie na nowe wektory ataków. Dane telemetryczne z dziesiątek tysięcy urządzeń w bankach spółdzielczych są agregowane i analizowane w czasie rzeczywistym w zintegrowanym systemie monitorującym. Analiza ta pozwala na wykrycie wczesnych sygnałów ataku (np. sondowania sieci, nietypowej aktywności) zanim atak rozwinie się w pełnoskalowy incydent. Wykrycie nawet niewielkiego incydentu w jednym banku spółdzielczym automatycznie wzmacnia ochronę pozostałych – każdy bank spółdzielczy jest chroniony doświadczeniem i reakcją na incydenty z pozostałych banków zrzeszenia. Wzajemna wymiana informacji i doświadczeń jest tu bezcenna.

SOC SGB to przede wszystkim maksymalizacja dostępności i jakości specjalistycznych kompetencji, przy jednoczesnej redukcji kosztów.



W świecie, w którym banki i ich klienci są codziennie atakowani, a cyberprzestrzeń jest polem bitwy, kluczem do przetrwania i rozwoju jest zjednoczenie sił.

„Najważniejszą korzyścią jest możliwość skonsolidowania kompetencji eksperckich w jednym miejscu. SOC SGB to kamień milowy w rozwoju zrzeszenia SGB, gwarantujący większą odporność na współczesne zagrożenia. Jesteśmy dumni z osiągniętego rezultatu i z niecierpliwością patrzymy w przyszłość, kontynuując wspólną pracę nad dalszym wzmacnianiem cyberbezpieczeństwa. Razem zbudowaliśmy bezpieczniejszą przyszłość dla naszych klientów i całej grupy SGB. Jesteśmy gotowi na nowe wyzwania!" ●

Banki spółdzielcze muszą konsekwentnie podnosić swoją efektywność organizacyjną poprzez wdrażanie nowych technologii cyfrowych oraz zwiększać poziom cyfryzacji produktów i kanałów dostępu do usług.

Cyberbezpieczeństwo, to gra zespołowa

Rozmowa z **Krzysztofem Dąbrowskim**,
dyrektorem zarządzającym Pionem Bezpieczeństwa UKNF

W jaki sposób UKNF ocenia różnice w poziomie zaawansowania technologicznego i kompetencyjnego między bankami komercyjnymi, a spółdzielczymi? Czy w ogóle one występują?

Oba segmenty bankowości, zarówno spółdzielczy jak i komercyjny, mają swoją specyfikę wynikającą z genezy ich powstania, modelu działania oraz znaczenia poszczególnych kanałów kontaktu z klientem. Banki spółdzielcze w większym stopniu stawiają na relacyjność i bezpośrednią obsługę, funkcjonują lokalnie i budują swoją przewagę poprzez wzmacnianie zaufania. Jednocześnie współczesna struktura produktów i usług finansowych oferowanych klientom nie różni się już istotnie między tymi dwiema grupami. W praktyce oznacza to, że również banki spółdzielcze muszą konsekwentnie podnosić swoją efektywność organizacyjną poprzez wdrażanie nowych technologii cyfrowych oraz zwiększać poziom cyfryzacji produktów i kanałów dostępu do usług. Idzie za tym szersze wykorzystanie technologii i narzędzi, które są standardem w bankowości komercyjnej.

Jakie są kluczowe oczekiwania UKNF wobec zrzeszeń banków spółdzielczych? Pytam w kontekście budowania jednolitych i scentralizowanych mechanizmów cyberbezpieczeństwa dla całej Grupy SGB.

Współcześnie rośnie skala wykorzystywania technologii cyfrowych w procesach wewnątrz podmiotów finansowych oraz postępuje cyfryzacja usług świadczonych ich klientom. Z drugiej strony dynamicznie zmienia się krajobraz cyberzagrożeń. W tym kontekście nietrudno dostrzec, że im większy potencjał kapitałowy, ludzki, techniczny i organizacyjny, tym łatwiej sprostać nowym wyzwaniom.

Ponadto cyberbezpieczeństwo na poziomie adekwatnym do ryzyk operacyjnych związanych z działalnością bankową, wymaga coraz większych nakładów i kompetencji. To wszyst-

FOT. UKNF

ko sprawia, że centralizacja procesów cyberbezpieczeństwa oraz budowanie spójnych procedur, a nawet struktur takich jak SOC (Security Operations Center), jest właściwym kierunkiem, który realnie zwiększa cyberodporność poszczególnych członków Grupy, a jednocześnie stwarza szansę na uzyskanie efektywności ekonomicznej.

Z perspektywy nadzoru finansowego, dbającego przecież o stabilność rynku finansowego, konsolidacja mechanizmów cyberbezpieczeństwa przynosi na tyle duże systemowe korzyści, że przewyższają one pewien wzrost ryzyka koncentracji.

Czyli konieczne jest centralizowanie mechanizmów cyberbezpieczeństwa w zrzeszeniach banków spółdzielczych?

Tak. Kluczowe oczekiwania UKNF wobec zrzeszeń banków spółdzielczych dotyczą stopniowego budowania jednolitych i bardziej scentralizowanych mechanizmów cyberbezpieczeństwa. Taki kierunek powinien wzmacniać zdolność całej

Centralizacja procesów cyberbezpieczeństwa oraz budowanie spójnych procedur, a nawet struktur takich jak SOC (Security Operations Center), jest właściwym kierunkiem, który realnie zwiększa cyberodporność poszczególnych członków Grupy, a jednocześnie stwarza szansę na uzyskanie efektywności ekonomicznej.

Grupy do reagowania na szybko zmieniające się zagrożenia. Choć centralizacja wiąże się z pewnym ryzykiem koncentracji, nadzór ocenia ją jako rozwiązanie uzasadnione, ponieważ pozwala lepiej koordynować działania i ujednolicać standardy ochrony.

Zasadne jest zapewnienie spójnego podejścia do zarządzania ryzykiem ICT. Powinno ono opierać się na wspólnych procedurach, jednolitych usługach bezpieczeństwa oraz konsekwentnym wdrażaniu wymogów DORA. W szczególności w obszarze zarządzania incydentami, wymiany informacji i testowania odporności. Dzięki temu cała Grupa może osiągnąć bardziej stabilny i przewidywalny poziom bezpieczeństwa operacyjnego.

Równocześnie UKNF zwraca uwagę na konieczność systematycznej analizy ryzyka oraz rozwijania zdolności operacyjnych, które obejmują zarówno odpowiednie kompetencje techniczne, jak i zdolność do sprawnego reagowania na incydenty w modelu współdzielonej infrastruktury. W praktyce oznacza to jasne określenie ról i odpowiedzialności w zrzeszeniu, podniesienie poziomu dojrzałości w zakresie nadzoru nad dostawcami ICT, konsolidację wiedzy o podatnościach oraz tworzenie wspólnych rozwiązań w obszarze monitorowania i detekcji. Nadzór oczekuje także systematycznego inwestowania w edukację i świadomość zarówno pracowników, jak i klientów, co jest niezbędnym elementem ograniczania skuteczności ataków socjotechnicznych. W opinii UKNF centralizacja w tych obszarach powinna być traktowana nie jako cel sam w sobie, lecz jako naturalny etap wzmacniania wspólnej odporności operacyjnej w zrzeszeniach banków spółdzielczych.

Czy UKNF widzi potrzebę stworzenia w Grupie SGB wspólnego programu ćwiczeń i testów odporności cyfrowej, obejmującego wszystkie podmioty zrzeszone?

Z perspektywy nadzoru finansowego stworzenie wspólnego i spójnego programu testów odporności cyfrowej przez banki spółdzielcze wraz z bankiem zrzeszającym należy ocenić jako

rozwiązanie zdecydowanie korzystne i wzmacniające stabilność całego sektora. Banki spółdzielcze funkcjonują w modelu wysokiej współzależności operacyjnej, a usługi często świadczone są przez wspólnych dostawców. W praktyce oznacza to, że incydent dotykający jednego podmiotu bardzo szybko może mieć konsekwencje dla pozostałych, a skuteczna reakcja wymaga spójnych procedur, jednolitych zasad komunikacji oraz przećwiczonej koordynacji działań z bankiem zrzeszającym.

W opinii UKNF centralizacja w tych obszarach powinna być traktowana nie jako cel sam w sobie, lecz jako naturalny etap wzmacniania wspólnej odporności operacyjnej w zrzeszeniach banków spółdzielczych.

Wspólny program ćwiczeń pozwala na przeprowadzenie testów obejmujących obszary, które mają kluczowe znaczenie dla bezpieczeństwa i ciągłości działania banków spółdzielczych. Szczególnie dotyczy to usług płatniczych, które są nie tylko najbardziej wrażliwym obszarem działalności banków,

Rola banku zrzeszającego w koordynowaniu reakcji na poważne incydenty bezpieczeństwa może w naturalny sposób zmierzać w kierunku większej centralizacji, co nadzór ocenia jako podejście spójne, zarówno z charakterem działania zrzeszeń, jak i z wymaganiami DORA.

ale również tym, w którym wszelkie zakłócenia są natychmiast odczuwalne przez klientów. Dzięki ćwiczeniom możliwe jest sprawdzenie, jak cały system reaguje na scenariusze związane z opóźnieniami w realizacji przelewów czy problemami z płatnością. Testowanie tych elementów w ramach jednolitego programu pozwala ocenić, czy ścieżki komunikacji i eskalacji są spójne, a bank zrzeszający jest w stanie właściwie koordynować działania naprawcze, jednocześnie dostarczając bankom spółdzielczym wiarygodnych informacji operacyjnych.

Jaka jest oczekiwana rola i odpowiedzialność SGB-Banku w koordynowaniu reakcji na poważne incydenty bezpieczeństwa, które dotyczą Banków Spółdzielczych SGB?

Rola banku zrzeszającego w koordynowaniu reakcji na poważne incydenty bezpieczeństwa może w naturalny sposób zmierzać w kierunku większej centralizacji, co nadzór ocenia jako podejście spójne zarówno z charakterem działania zrzeszeń, jak i z wymaganiami DORA. W modelu opartym na współdzielonej infrastrukturze i jednolitych rozwiązaniach ICT scentralizowana koordynacja ułatwia uporządkowanie informacji, ocenę wpływu incydentu na poszczególne podmioty oraz zapewnia większą jednolitość procedur reagowania. Takie podejście zmniejsza ryzyko rozbieżnych działań i pozwala szybciej odtworzyć pełny obraz sytuacji, co w strukturach wielopodmiotowych jest szczególnie ważne.

W tym ujęciu bank zrzeszający może odpowiadać za analizę incydentu, wsparcie dla podmiotu dotkniętego zdarzeniem oraz za sprawną wymianę informacji w ramach ekosystemu cyberbezpieczeństwa, zgodnie z obowiązkami wynikającymi z DORA. Obejmuje to zarówno konsolidację danych o przebiegu zdarzenia, jak i przekazywanie istotnych informacji innym bankom spółdzielczym oraz utrzymanie kontaktu z właściwymi instytucjami, w tym CSIRT KNF. Centralizacja doświadczeń i wiedzy o incydentach sprzyja budowaniu bardziej spójnych standardów bezpieczeństwa, a także wspiera rozwój jednolitego poziomu odporności cyfrowej w całej sieci banków spółdzielczych, co nadzór postrzega jako kierunek uzasadniony i naturalnie wynikający z modelu działania zrzeszeń.

Biorąc pod uwagę aktualne trendy zagrożeń (np. socjotechnika, ransomware), jakie są trzy najważniejsze obszary cyberbezpieczeństwa, na które Grupa SGB powinna przeznaczyć najwięcej zasobów w najbliższych 2-3 latach, aby wzmocnić swoją wspólną odporność?

W perspektywie najbliższych 2-3 lat trzy obszary wydają się kluczowe dla wzmocnienia wspólnej odporności banków spółdzielczych i banku zrzeszającego. Pierwszym z nich jest ochrona przed atakami ransomware i wyciekami danych, które pozostają jednym z najbardziej szkodliwych i kosztownych typów incydentów. Skuteczna obrona wymaga nie tylko odpowiednich zabezpieczeń technicznych, lecz także właściwego ujęcia zarządzania ryzykiem ICT w całym systemie zarządzania organizacją oraz stałej analizy cyfrowego ryzyka operacyjnego. Podstawowe znaczenie ma również edukacja pracowników i klientów, ponieważ to właśnie socjotechnika pozostaje jednym z głównych wektorów ataku, a jej skuteczność często niweluje nawet dobrze zaprojektowane zabezpieczenia.

Drugim priorytetem powinno być wzmocnienie nadzoru nad dostawcami ICT i szeroko pojęte bezpieczeństwo łańcucha dostaw, zgodnie z podejściem przewidzianym w DORA. W modelu zrzeszeniowym wiele usług świadczonych jest przez dostawców zewnętrznych. Oznacza to, że incydent po stronie jednego z nich może oddziaływać na cały ekosystem. Konieczne jest więc zarówno precyzyjne zarządzanie ryzykiem koncentracji, jak i systematyczna ocena odporności dostawców, testowanie ich zdolności do reagowania na incydenty oraz budowanie mechanizmów kontroli, które pozwalają szybko identyfikować zagrożenia pojawiające się w łańcuchu usług. DORA jednoznacznie wzmacnia znaczenie tego obszaru, podkreślając, że organizacje muszą mieć realny nadzór nad podmiotami świadczącymi usługi ICT oraz odpowiednio dokumentować i testować ich gotowość operacyjną.

Trzeci obszar dotyczy zagrożeń związanych z wykorzystaniem sztucznej inteligencji do prowadzenia ataków. Choć dziś są one w dużej mierze zapowiedzią przyszłych trendów, rozwijają się na tyle szybko, że w perspektywie kilku lat mogą stać się istotnym problemem operacyjnym. Mogą obejmować zarówno precyzyjne kampanie phishingowe oparte na deepfake'ach głosu i obrazu, jak i automatyzację analiz podatności. Odpowiedzią na te wyzwania powinny być inwestycje w zaawansowane mechanizmy detekcji anomalii, rozwój procesów analitycznych i kompetencji zespołów odpowiedzialnych za bezpieczeństwo. Wspólne podejście banków spółdzielczych i banku zrzeszającego do tych trzech obszarów, oparte na spójnych standardach i współdzielonych doświadczeniach, może istotnie wzmocnić odporność całego zrzeszenia na szybko zmieniające się zagrożenia.

Rozmawiał: Roman Szewczyk

Cyberoszuści przyspieszają. **Tak atakowali nas w 2025 roku**

Krzysztof Swoboda
Technical content manager w takaoto.pro

Rok 2025 przynosi bezprecedensowy wzrost cyberprzestępczości – od deepfake'ów generowanych przez AI po wyrafinowane ataki ransomware. Polska znalazła się na pierwszym miejscu na świecie pod względem liczby ataków ransomware, a straty z oszustw cyfrowych osiągają rekordowe poziomy. Jak zwiększyć swoje szanse na uniknięcie oszustwa?

Era deepfake'ów – gdy rzeczywistość staje się niemożliwa do zweryfikowania

Technologia deepfake w 2025 roku osiągnęła poziom, który jeszcze niedawno pasował bardziej do filmów science fiction niż do rzeczywistości. W pierwszym kwartale 2025 roku firmy na całym świecie straciły ponad 200 mln dolarów w wyniku oszustw z użyciem deepfake[1].

Przestępcy wykorzystują tę technologię w coraz bardziej wyrafinowany sposób. W 2023 r. w mediach społecznościowych na całym świecie udostępniono około 500 000 deepfake'ów filmów i nagrań głosowych, a prognozy wskazują, że do 2025 roku ich liczba może wzrosnąć nawet do 8 milionów.

Szczególnie niebezpieczny jest tzw. vishing głosowy, gdzie raport Pindrop wskazuje na wzrost aktywności związanej z głosowymi deepfake'ami o 680% w ciągu ostatniego roku[2].

Polska liderem ataków ransomware – alarmujące statystyki

Dane dotyczące ransomware w Polsce są już więcej niż alarmujące. Według raportów ESET, w pierwszej połowie 2025 roku Polska znalazła się na pierwszym miejscu na świecie pod względem liczby wykrytych ataków, odpowiadając za 6% wszystkich globalnych incydentów i wyprzedzając nawet Stany Zjednoczone[3].

Co gorsza, jedynie 59% polskich firm deklaruje korzystanie z oprogramowania zabezpieczającego, a zaledwie 19% zatrudnionych w Polsce rozumie pojęcie „ransomware". Szczególnie niepokojące jest wykorzystanie nowej techniki ClickFix, której „popularność" wzrosła aż o 517%, czyniąc ją drugim najpopularniejszym wektorem ataku po phishingu. Przestępcy podszywają się pod popularne narzędzia biznesowe, takie jak Microsoft Teams, wykorzystując niską świadomość pracowników.

Quishing, smishing, vishing – nowe oblicza tradycyjnego phishingu

Cyberprzestępcy nieustannie rozwijają i ulepszają dotychczas stosowane taktyki – to wielki wyścig z firmami dbającymi o cyberbezpieczeństwo, który zdaje się nie mieć końca. Obok tradycyjnego phishingu, dziś prym wiodą takie techniki, jak:

- Smishing (SMS-based phishing) – to oszustwa SMS-owe, czyli phishing realizowany przez wiadomości tekstowe, często podszywający się pod firmy kurierskie, urzędy czy banki. W 2024 roku zanotowano blisko 355 tysięcy zgłoszeń podejrzanych wiadomości SMS, co w porównaniu z ponad 221 tysiącami zgłoszeń w roku 2023 oznacza wzrost o 60%[4].
- Quishing – phishing z wykorzystaniem kodów QR, który staje się coraz większym zagrożeniem. Szacuje się, że ponad 100 milionów Amerykanów będzie używać swoich smartfonów do skanowania kodów QR do 2025 roku. Przestępcy umieszczają złośliwe kody QR w miejscach publicznych, na przykład na restauracyjnych stolikach, podszywając się pod menu czy promocje.
- Vishing – w tym scenariuszu atakujący dzwoni do ofiary, podszywając się pod bank, policję, technika IT lub członka rodziny. Coraz częściej wykorzystuje do tego syntetyczny, wygenerowany głos oraz zautomatyzowane platformy telefoniczne, dzięki czemu może wykonywać masowe kampanie na skalę globalną.

> Kluczowa jest edukacja i zachowanie podstawowych zasad cyfrowej higieny.

Oszustwa inwestycyjne w kryptowaluty – stara taktyka w nowej odsłonie

Rynek kryptowalut, który jeszcze w 2024 roku wydawał się już całkiem stabilny i dobrze zabezpieczony, znów stał się atrakcyjnym celem

1 https://www.securitymagazine.com/articles/101559-deepfake-enabled-fraud-caused-more-than-200-million-in-losses
2 https://www.pindrop.com/article/deepfake-fraud-could-surge/
3 https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h12025.pdf
4 https://www.nask.pl/aktualnosci/300-incydentow-dziennie-premiera-raportu-cert-polska-za-2024-rok

dla przestępców. Złodzieje odkopali starą, ale wciąż skuteczną taktykę, której używali kilka lat temu: tworzą fałszywe platformy inwestycyjne, których jedynym celem jest wyłudzenie środków. Myślisz, że na tak prostą zanętę nikt już się nie nabierze? Tylko w zeszłym roku, za sprawą działalności jednej, 9-osobowej grupy, z rynku wyparowało 600 milionów euro[5].

Jedynie 59% polskich firm deklaruje korzystanie z oprogramowania zabezpieczającego, a zaledwie 19% zatrudnionych w Polsce rozumie pojęcie „ransomware".

W Polsce problem również występuje, ale pojawia się tutaj dodatkowy „czynnik lokalny" – przestępcy wykorzystują wizerunki znanych osób, takich jak Robert Lewandowski czy Anna Lewandowska, do promowania fałszywych inwestycji. Okazuje się, że ta prosta taktyka może działać na internautów jak magnes.
Sam mechanizm jest bardzo prosty: ofiary są kierowane na fałszywe platformy, gdzie po dokonaniu pierwszego przelewu otrzymują dostęp do panelu pokazującego fikcyjne zyski. Gdy próbują wypłacić „zarobione" pieniądze, kontakt z oszustami się urywa.

Metoda „na wnuczka" w erze AI

To klasyczne oszustwo przeszło istną technologiczną metamorfozę. W 2025 roku przestępcy działają znacznie szerzej i sprytniej, wykorzystując deepfake audio do generowania głosu, który brzmi identycznie jak głos wnuczka, córki czy syna. Przestępcy nie ograniczają się już tylko do podszywania się pod członków rodziny – coraz częściej występują jako policjanci, prokuratorzy czy pracownicy instytucji samorządowych.

Ta technika doskonale pokazuje też, że szkoły, rodzice, ale też dzieci i osoby starsze, muszą szczególnie uważać na to, co umieszczają na Facebooku czy filmikach na YouTube czy TikToku. Kiedyś abstrakcyjne pojęcia, jak „kradzież twarzy" czy „kradzież głosu" są dziś dostępne praktycznie dla każdego. Wystarczy pobrać plik wideo, wyodrębnić ścieżkę audio i… mieć złe intencje. Reszta to formalność.
Potrzeba realnych zabezpieczeń systemowych, po stronie właścicieli mediów społecznościowych, ale też najzwyklejszej w świecie kalkulacji i myślenia o potencjalnych konsekwencjach upubliczniania zbyt wielu informacji w sieci. To realny problem, z tórym wszyscy – zarówno rodzice, przedsiębiorcy, jak i instytucje finansowe, będziemy musieli się zmierzyć.

Jak się bronić? Praktyczne wskazówki na 2025 i 2026 rok

Jeden fakt jest niepodważalny: kluczowa jest edukacja i zachowanie podstawowych zasad cyfrowej higieny. Przede wszystkim należy weryfikować każdą nieoczekiwaną prośbę o pieniądze czy dane, nawet jeśli wydaje się pochodzić od znanej osoby. W przypadku kodów QR zawsze należy sprawdzać adres URL przed wprowadzeniem jakichkolwiek danych.

Polska znalazła się na pierwszym miejscu na świecie pod względem liczby ataków ransomware, a straty z oszustw cyfrowych osiągają rekordowe poziomy.

Przedsiębiorstwa powinny regularnie szkolić pracowników – szacuje się, że ponad połowa (52%) zatrudnionych w Polsce nie uczestniczyła w żadnym szkoleniu z zakresu cyberbezpieczeństwa w ciągu ostatnich pięciu lat. To luka, którą przestępcy bezwzględnie wykorzystują[6].
Cyberprzestępczość w 2025 roku nie jest już problem pojedynczych hakerów, ale zorganizowanych grup dysponujących zaawansowanymi narzędziami AI. Grupy te często atakują nasz kraj zza wschodniej granicy, co wielu ekspertów uważa za kolejny etap wojny hybrydowej, z jaką zmaga się praktycznie cała wschodnia flanka NATO. A to oznacza, że zagrożenie raczej nie ustanie oraz że będzie ono miało charakter długotrwały i – niestety – zorganizowany.
Parafrazując słowa klasyka, wszystko wskazuje na to, że „lepiej już było", a nadchodzące lata będą wymagały od wszystkich internautów ogromnej czujności praktycznie na każdym etapie naszej cyfrowej aktywności: od publikowania zdjęć i wideo z wakacji w social mediach, przez płatności online, po ciągłą ekspozycję na dezinformację – zarówno w wymiarze ogólnokrajowym, jak i lokalnym. ●

5 https://www.bankinfosecurity.com/cryptohack-roundup-europol-busts-600m-euro-fraud-network-a-29947

6 https://polandinsight.com/polish-businesses-at-risk-41-lack-antivirus-protection-and-over-half-of-employees-untrained-in-cybersecurity-16364/#google_vignette

Oszustwo zaczyna się tam, gdzie kończy się czujność

Roma Śmigielska
SGB-Bank

Każdego dnia w banku spotykamy historie osób, które jeszcze rano były pewne, że nigdy nie padną ofiarą oszustwa. Wierzyły, że „zawsze sprawdzają", „nigdy nie podają danych" i „doskonale wiedzą, z kim rozmawiają". A jednak wystarczył jeden telefon, jedno kliknięcie, jedna chwila nieuwagi.

Właśnie tak zaczyna się większość oszustw

W Zrzeszeniu SGB korzystamy z zaawansowanych narzędzi i technologii, które działają bez przerwy. Jedną z kluczowych usług jest FDS – nowoczesne rozwiązanie, które monitoruje transakcje klientów i wychwytuje podejrzane działania. Dzięki niemu w tym roku zatrzymaliśmy już ponad 36 milionów złotych, które miały trafić do przestępców. Mimo skuteczności FDS jedno pozostaje niezmienne – największe ryzyko kryje się w ludzkich decyzjach. Oszuści nie atakują systemów – oni atakują emocje. Wykorzystują presję czasu, stres, poczucie zaufania. Jeden moment rozproszenia wystarczy, by wykorzystali okazję. Tak właśnie zaczyna się większość oszustw.

Wystarczy obietnica szybkiego zysku i profesjonalnie przygotowana historia. Tak działają oszustwa inwestycyjne.

Twoje konto jest właśnie atakowane

Jednym z częstych scenariuszy jest telefon od osoby podającej się za pracownika banku. Rozmowa brzmi profesjonalnie, a przekaz jest jasny: „Twoje konto jest właśnie atakowane, musisz działać natychmiast". Dalej pojawia się instrukcja – może to być instalacja aplikacji rzekomo chroniącej bankowość, podanie danych do logowania albo wykonanie przelewu na „konto techniczne" w celu zabezpieczenia pieniędzy. Coraz częściej oszuści stosują dodatkowe sztuczki, żeby wyglądać wiarygodnie. Jedną z nich jest wysyłanie SMS-ów w trakcie rozmowy. Takie wiadomości mają potwierdzić, że klient faktycznie rozmawia z pracownikiem banku. Każdy krok prowadzi do przejęcia kontroli nad finansami ofiary. Jak się przed tym bronić? Najważniejsze jest, żeby zachować spokój i nie działać pod presją. Pracownicy banku nigdy nie proszą przez telefon o instalowanie dodatkowych aplikacji, podawanie

danych do logowania ani wykonywanie przelewów na „techniczne” konta. Jeśli pojawia się informacja, że pieniądze są zagrożone, najlepiej zakończyć rozmowę i samemu zadzwonić na oficjalną infolinię banku.

Oszustwa inwestycyjne

Telefony od „pracowników banku” to tylko jedna z metod, którą wykorzystują oszuści. Niestety, na tym nie kończą się ich pomysły. Jeszcze bardziej podstępne są scenariusze, w których klient sam, z pełnym przekonaniem, przekazuje swoje pieniądze przestępcom. Jak to możliwe? Wystarczy obietnica szybkiego zysku i profesjonalnie przygotowana historia. Tak działają oszustwa inwestycyjne - pułapki, które zaczynają się od niewinnej reklamy w internecie, a kończą na utracie oszczędności życia. Wyobraźmy sobie klienta, który przegląda internet i trafia na reklamę obiecującą „pewny zysk” w krótkim czasie. Oferta wygląda profesjonalnie – jest logo znanej firmy, wykresy, opinie „zadowolonych inwestorów”. Wystarczy zostawić numer telefonu, aby dowiedzieć się więcej. Kilka minut później dzwoni „doradca inwestycyjny”. Rozmowa jest pełna fachowych terminów, a ton głosu budzi zaufanie. Klient słyszy, że to niepowtarzalna okazja, a w kilka tygodni jego pieniądze mogą znacząco się pomnożyć. Aby zacząć, wystarczy wykonać przelew na wskazane konto i zalogować się do platformy inwestycyjnej. Na ekranie klient widzi, jak jego „inwestycja” rośnie. W rzeczywistości to tylko symulacja przygotowana przez oszustów. Klient jest przekonany, że zarabia, więc chętnie wpłaca kolejne środki. Często bank zatrzymuje taki przelew z powodów bezpieczeństwa. Wtedy klient dzwoni na infolinię i… potwierdza transakcję. Dlaczego? Bo oszust wcześniej uprzedził go, że „bank będzie próbował zablokować inwestycję, bo chce, żebyś trzymał pieniądze u nich. Oni zarabiają na twoich oszczędnościach”. Pracownik podczas rozmowy, widząc ryzyko, zadaje dodatkowe pytania: czy klient nie trafił na reklamę inwestycji w internecie, czy ktoś się z nim kontaktował w tej sprawie, czy zna odbiorcę przelewu. To ma wzbudzić czujność klienta, ale manipulacja nadal działa. Klient jest pewny swojego, bo oszust przygotował go na każdą wątpliwość. Jak więc uniknąć takiej pułapki? Kluczowe jest zrozumienie, że żadna legalna instytucja finansowa nie obiecuje „pewnego zysku” w krótkim czasie. Jeśli oferta brzmi zbyt dobrze, by była prawdziwa najprawdopodobniej jest oszustwem. Zanim przekażesz swoje pieniądze, sprawdź wiarygodność firmy w oficjalnych rejestrach, np. na stronie Komisji Nadzoru Finansowego. Nigdy nie ufaj reklamom w mediach społecznościowych ani rozmowom telefonicznym z nieznajomymi „doradcami”. Warto też pamiętać, że bank, który blokuje przelew, nie robi tego „z chciwości”, ale w trosce o bezpieczeństwo klienta. Jeśli pojawiają się wątpliwości – zatrzymaj się, skontaktuj z bankiem przez oficjalne kanały i porozmawiaj z kimś zaufanym. Oszuści bazują na emocjach i pośpiechu, dlatego najskuteczniejszą bronią jest czas i zdrowy rozsądek.

> Oszustwo nie zaczyna się wtedy, gdy pieniądze znikają z konta. Ono zaczyna się znacznie wcześniej.

Oszuści bazują na emocjach i pośpiechu

Choć te historie są różne, mają wspólne elementy. Oszuści zawsze budują atmosferę pośpiechu. Przekonują ofiarę, że „musi działać teraz”, bo inaczej pieniądze znikną albo okazja przepadnie. W takich sytuacjach człowiek przestaje myśleć racjonalnie i robi dokładnie to, czego oczekują przestępcy. Dlatego mówiąc o bezpieczeństwie, zawsze powtarzam

> Oszuści nie atakują systemów – oni atakują emocje.

jedno: oszustwo nie zaczyna się wtedy, gdy pieniądze znikają z konta. Ono zaczyna się znacznie wcześniej - w chwili, kiedy ktoś wzbudza w nas strach, pośpiech albo nadzieję na szybki zysk. I właśnie wtedy potrzebna jest czujność. Bo kiedy kończy się czujność, zaczyna się oszustwo. A tych kilka sekund namysłu naprawdę może uratować dorobek całego życia. ●

Cyberhigiena na co dzień: **proste nawyki, które chronią klientów i bank**

Piotr Dunder
SGB-Bank

W dzisiejszym świecie, gdzie bankowość odbywa się głównie online, a smartfon stał się naszym osobistym centrum finansowym, cyfrowe bezpieczeństwo przestało być abstrakcyjnym problemem informatyków. Stało się osobistą odpowiedzialnością każdego z nas. Tak jak regularnie myjemy ręce, by chronić się przed zarazkami, tak samo musimy dbać o naszą „cyberhigienę", aby chronić pieniądze, dane i zaufanie do systemu bankowego.

Banki inwestują ogromne środki w zaawansowane systemy zabezpieczeń. Stosują szyfrowanie, biometrię i ciągłe monitorowanie transakcji. Jednak najsłabszym ogniwem w łańcuchu bezpieczeństwa często okazuje się człowiek. Nawet najsolidniejszy zamek nie ochroni domu, jeśli właściciel zostawi klucz pod wycieraczką. Twoje proste, codzienne nawyki mają realny wpływ na to, czy przestępca uzyska dostęp do Twojego konta – i czy bank poniesie straty. Oto praktyczne zasady cyberhigieny, które każdy klient banku powinien wprowadzić w życie natychmiast.

Zasada 1: Siła tkwi w haśle

Hasło to pierwsza i najczęściej jedyna linia obrony dostępu do Twoich pieniędzy. Niestety, wiele osób używa haseł, które hakerzy mogą złamać w ułamku sekundy, lub co gorsza – używa tego samego hasła do banku, poczty i konta na portalu społecznościowym.

Jak dbać o hasła?

- Długość ma znaczenie: Dobre hasło powinno mieć minimum 12 znaków. Im dłuższe, tym lepiej.
- Kompozycja to podstawa: Używaj kombinacji dużych i małych liter, cyfr oraz znaków specjalnych (np. !@#$%^). Unikaj prostych słów, imion, dat urodzenia czy popularnych cytatów.
- Unikalność to bezpieczeństwo: Nigdy nie używaj tego samego hasła w banku co na innych stronach. Jeśli hakerzy zdobędą hasło z mniej bezpiecznego serwisu (np. forum dyskusyjnego), będą próbowali go użyć wszędzie indziej. To się nazywa atak typu credential stuffing.
- Menedżer haseł – Twój cyfrowy sejf: Zamiast zapisywać hasła na kartkach, używaj profesjonalnego menedżera haseł (np. LastPass, 1Password, Bitwarden). To zaszyfrowane programy, które bezpiecznie przechowują hasła i potrafią generować silne, unikalne kombinacje dla każdej usługi.

Zasada 2: Włącz Wielostopniową Weryfikację (2FA/MFA)

Jeśli hasło jest kluczem, to weryfikacja dwustopniowa (ang. Two-Factor Authentication, 2FA lub MFA – Multi-Factor Authentication) jest drugim, niezależnym zamkiem. Po wpisaniu poprawnego hasła, system prosi o dodatkowy dowód Twojej tożsamości.

Najczęściej tym drugim czynnikiem jest:

1. Kod SMS: Chociaż wygodny, jest uznawany za mniej bezpieczny niż pozostałe metody.

Banki chronią
Twoje pieniądze,
ale bezpieczeństwo
zaczyna się od Ciebie.

2. Aplikacja uwierzytelniająca (Token): Takie aplikacje jak Google Authenticator, Microsoft Authenticator, które zmieniają się co 30-60 sekund. To obecnie najbezpieczniejsza i zalecana metoda.
3. Klucze sprzętowe: Fizyczne urządzenia (np. YubiKey) wymagające dotknięcia – najbezpieczniejsza opcja.

Zawsze włączaj 2FA, zarówno w banku, poczcie e-mail, jak na kontach społecznościowych i w każdym serwisie, który na to pozwala. To najprostszy sposób, by zniwelować ryzyko przejęcia konta, nawet jeśli Twoje hasło wpadnie w niepowołane ręce.

Zasada 3: Bezpieczeństwo w sieci i na telefonie

Banki oferują dziś aplikacje mobilne – są one zaprojektowane tak, by były bezpieczniejsze niż korzystanie z bankowości przez przeglądarkę na komputerze. Musimy jednak zadbać o otoczenie, w którym z nich korzystamy:

- Aktualizuj! Zarówno Twój komputer (Windows/macOS) jak i telefon (Android/iOS)

oraz wszystkie zainstalowane aplikacje (szczególnie bankową) muszą być na bieżąco aktualizowane. Aktualizacje to nie tylko nowe funkcje, ale przede wszystkim łatki bezpieczeństwa, które zamykają luki wykryte przez cyberprzestępców. Nie odkładaj aktualizacji „na później”.

- Używaj oprogramowania antymalware. Na komputerze stacjonarnym zawsze korzystaj z aktualnego oprogramowania antywirusowego/antymalware. Chociaż systemy mobilne są generalnie bezpieczniejsze, dodatkowa ochrona na Androidzie również bywa zalecana.
- Unikaj publicznego Wi-Fi. Nigdy nie loguj się do banku ani nie dokonuj transakcji, gdy jesteś połączony z niezabezpieczoną, publiczną siecią Wi-Fi (np. w kawiarni, na lotnisku, w hotelu). Hakerzy mogą łatwo przechwycić Twoje dane w takiej sieci. Jeśli musisz skorzystać z bankowości poza domem, użyj własnego pakietu danych komórkowych (LTE/5G) – to znacznie bezpieczniejsze.
- Instaluj z pewnego źródła. Aplikacje, w tym bankową, pobieraj wyłącznie z oficjalnych sklepów (Google Play Store, Apple App Store). Uważaj na linki SMS lub e-mail kierujące do pobrania rzekomej „nowej aplikacji banku”.

Tak jak regularnie myjemy ręce, by chronić się przed zarazkami, tak samo musimy dbać o naszą „cyberhigienę”, aby chronić pieniądze, dane i zaufanie do systemu bankowego.

Zasada 4: Rozpoznaj i zgłoś oszustwo (Phishing)

Phishing to najpopularniejsza metoda ataku, w której przestępcy podszywają się pod bank, urzędy lub operatorów, by wyłudzić od Ciebie dane (hasło, login, numer karty, kod BLIK). Przestępcy wykorzystują ludzką ciekawość, pośpiech lub strach.

Jak działają oszustwa?

- Poczta e-mail/SMS: Otrzymujesz wiadomość o rzekomej blokadzie konta, konieczności dopłaty do przesyłki kurierskiej, prośbie o zwrot nadpłaty czy udziale w pilnej weryfikacji danych. Zawsze zawierają link, który prowadzi do fałszywej strony logowania łudząco podobnej do strony banku.
- Telefony (Vishing): Oszust dzwoni, podając się za pracownika banku lub policjanta, informując o podejrzanym przelewie lub ataku hakerskim na Twoje konto. Prosi o zainstalowanie programu do zdalnej pomocy (np. AnyDesk, TeamViewer) lub o podanie danych do logowania, by „ochronić” Twoje pieniądze.
- Fałszywe inwestycje/SMS-y BLIK: Kuszenie łatwym zarobkiem lub prośba znajomego na komunikatorze o podanie kodu BLIK.

Hasło to pierwsza i najczęściej jedyna linia obrony dostępu do Twoich pieniędzy.

Jak się chronić?

1. Zawsze sprawdzaj adres URL: Zanim się zalogujesz, upewnij się, że adres strony w przeglądarce jest poprawny. Szukaj symbolu kłódki przy adresie.
2. Pamiętaj: bank nigdy nie prosi o tożsamość: Bank nigdy nie poprosi Cię przez telefon, SMS czy e-mail o:
   - całe hasło i login,
   - instalację dodatkowego oprogramowania na telefonie lub komputerze,
   - podanie pełnego numeru karty płatniczej z kodem CVV/CVC,
   - wykonanie „testowego” przelewu lub wygenerowanie i podanie kodu BLIK w celu weryfikacji tożsamości.
3. Wątp i weryfikuj: Jeśli masz najmniejszą wątpliwość co do wiadomości lub telefonu, rozłącz się lub nie klikaj w link. Zadzwoń na oficjalną infolinię swojego banku (znajdź numer na oficjalnej stronie banku, nie korzystaj z numeru podanego w podejrzanym SMS-ie) i zweryfikuj informację.
4. Zgłaszaj incydenty: Jeśli zorientujesz się, że padłeś ofiarą oszustwa, natychmiast skontaktuj się z bankiem i poinformuj o tym policję.

Wzajemna odpowiedzialność

Cyberhigiena to proces, który chroni nie tylko Ciebie, ale i cały ekosystem bankowy. Kiedy stosujesz te proste nawyki, zwiększasz swoje bezpieczeństwo i jednocześnie redukujesz ryzyko strat dla banku, co ostatecznie przekłada się na niższe koszty i wyższy poziom zaufania.

Banki chronią Twoje pieniądze, ale bezpieczeństwo zaczyna się od Ciebie. Nie oddawaj kluczy złodziejom – stosuj mocne hasła i włącz 2FA/MFA. W cyfrowym świecie ostrożność to Twoja najlepsza inwestycja. ●

Jak bankować bez stresu?

Nowa era bezpieczeństwa w SGB Mobile

Rafał Bandurski
SGB-Bank

Smartfon stał się naszym osobistym centrum dowodzenia – obsługujemy nim finanse, zakupy i codzienne obowiązki. Im więcej działań przenosimy do świata online, tym większe znaczenie ma bezpieczeństwo. Cyberprzestępcy nie śpią, a ich metody stają się coraz bardziej wyrafinowane. Najnowsze zmiany w aplikacji SGB Mobile to przykład, jak technologia wspiera ochronę środków naszych klientów.

Biometria behawioralna - inteligentna ochrona w tle

Podstawą nowoczesnej ochrony jest biometria behawioralna. To technologia, która wychodzi poza standardowe metody weryfikacji. Już na etapie logowania do SGB Mobile system rozpoznaje użytkownika. W tym celu bada sposób interakcji z ekranem, np. tempo i nacisk przy wpisywaniu danych. Nieprawidłowości są wychwytywane w ułamku sekundy, a reakcja systemu zapewnia maksymalną ochronę finansów. Co istotne, mechanizm działa w tle, bez dodatkowych kroków po stronie klienta. Cały czas sprawdzamy tożsamość użytkownika, aby w razie zagrożenia od razu podjąć działania i jednocześnie zapewnić wygodne korzystanie z aplikacji.

Podstawą nowoczesnej ochrony jest biometria behawioralna. Już na etapie logowania do SGB Mobile system rozpoznaje użytkownika.

Technologia, która widzi więcej

Biometria behawioralna to dopiero początek. W aplikacji SGB Mobile dodaliśmy również nowe narzędzia do analizy ryzyka, które działają jak dodatkowe tarcze ochronne. Bierzemy pod uwagę wiele czynników związanych z urządzeniem i aktywnością użytkownika, aby wykrywać anomalie i zatrzymać oszustów, zanim zdążą wyrządzić szkody. Wszystko odbywa się w tle, bez ingerencji użytkownika, ale z realnym wpływem na bezpieczeństwo. Dotychczasowe przypadki wskazują, że te rozwiązania skutecznie chronią klientów w sytuacjach, gdy są narażeni na manipulację lub próbę przejęcia środków. To dowód na to, że technologia może być sprzymierzeńcem w walce z socjotechniką, która dziś jest jednym z największych wyzwań w bankowości.

Dzięki tym zmianom aplikacja SGB Mobile staje się jednym z najbardziej zaawansowanych narzędzi w zakresie bezpieczeństwa w Zrzeszeniu SGB. To kolejny krok w realizacji naszej strategii - zapewnić klientom najwyższy poziom ochrony, bez kompromisów w wygodzie korzystania z usług. Sukces tego projektu to efekt ścisłej współpracy zespołów odpowiedzialnych za bezpieczeństwo transakcji oraz rozwój bankowości mobilnej, które wspólnie tworzą rozwiązania odpowiadające na najbardziej aktualne zagrożenia. ●

Ekspertki z SGB ostrzegają

Klaudia Olszak, Anita Szyndlar
SGB-Bank

Bezpieczeństwo finansowe to codzienna walka z tym, czego nie widać gołym okiem – z praniem pieniędzy, oszustwami i coraz bardziej wyrafinowanymi próbami manipulacji.

W SGB-Banku działają zespoły, które czuwają nad tym, by pieniądze klientów były bezpieczne. Analizowanie transakcji, wykrywanie podejrzanych schematów i szybka reakcja, zanim oszuści zdążą sięgnąć po cudze środki – to codzienność pracy w obszarze bezpieczeństwa finansowego.

To też praca zespołowa różnych obszarów. W SGB-Banku czuwają nad nim m.in. Anita Szyndlar, ekspertka AML w obszarze zarządzania ryzykiem, oraz Klaudia Olszak, ekspertka ds. cyberbezpieczeństwa.

Anita wraz z zespołem, zajmują się przeciwdziałaniem praniu pieniędzy – monitorują transakcje, weryfikują klientów i zgłaszają podejrzane przypadki, aby środki pochodzące z nielegalnych źródeł nie trafiły do obrotu finansowego.

Natomiast Klaudia z zespołem ds. antyfraud, odpowiada za wykrywanie i zapobieganie oszustwom finansowym. Jej praca polega na analizie nietypowych transakcji, wychwytywaniu sygnałów ostrzegawczych i szybkim reagowaniu na próby wyłudzeń.

Sprawdźmy jak wygląda ta codzienność. Na czym polega tzw. oszustwo nigeryjskie?

W zespole antyfraudowym codzienność to analiza nietypowych transakcji, wychwytywanie sygnałów ostrzegawczych i szybka reakcja na próby wyłudzeń. Specjaliści muszą być czujni, bo oszuści stosują coraz bardziej wyrafinowane metody - od fałszywych inwestycji po klasyczne schematy manipulacji, takie jak oszustwo metodą „na księcia”, znane również jako oszustwo nigeryjskie. To jeden z najstarszych i najbardziej rozpoznawalnych schematów w sieci, który mimo upływu lat wciąż jest aktualny. Historia zwykle zaczyna się niewinnie na czatach, forach lub przez wiadomości e-mailowe, możemy poznać osobę podającą się za amerykańskiego żołnierza na misji, nigeryjskiego księcia, bogatego biznesmena lub inną postać. Opowieść brzmi wiarygodnie, a jej celem jest jedno - wzbudzić zaufanie i poczucie wyjątkowości. Internetowa znajomość się rozwija, relacja staje się coraz silniejsza.

Nasz „wymarzony książę” – a w rzeczywistości oszust – zdobywa zaufanie powoli, bez pośpiechu, snując plany na przyszłość, obiecując wspólne życie lub wielką przyjaźń. W pewnym momencie pojawia się prośba o pomoc. Na początku to drobna suma na „pilny problem”. I tu rodzi się pytanie: skoro to książę, milioner czy wpływowy biznesmen, po co mu nasze pieniądze? Odpowiedź jest zawsze gotowa – środki są chwilowo zamrożone, konto zablokowane, a inwestycja jest pilna. Oszust przekonuje, że to tylko tymczasowa trudność, która wkrótce się skończy, a wtedy czeka nas ogromna nagroda. Brzmi wiarygodnie, bo przecież wcześniej zdobył nasze zaufanie, snując plany na przyszłość i zapewniając o szczerości swoich intencji.

To początek spirali. Po pierwszej wpłacie pojawiają się kolejne „koszty” podatki, dokumenty, opłaty za prawników. Każdy przelew ma być „ostatnim krokiem”, lecz w rzeczywistości otwiera drogę do kolejnych żądań. Oszust wprowadza presję czasu i prosi o tajemnicę, aby odciąć ofiarę od pomocy. Gdy pojawiają się wątpliwości, wymyśla nowe powody, by żądać pieniędzy. Kiedy wyłudzi od ofiary wszystkie pieniądze, znika bez śladu w czeluściach internetu. Na pytanie, dlaczego ofiary wpadają w tę pułapkę, odpowiedź jest

> Ofiarami oszustw, takich jak na przystojnego oficera armii amerykańskiej czy nigeryjskiego księcia, najczęściej padają kobiety.

bardziej złożona niż zwykła nieostrożność. Często są to osoby samotne, spragnione bliskości, które szukają miłości w świecie, gdzie coraz trudniej ją znaleźć. Oszuści wykorzystują tę potrzebę, budując poczucie zaufania i bezpieczeństwa, a gdy relacja się zacieśnia, wstyd i strach przed przyznaniem się do błędu sprawiają, że ofiary angażują się coraz bardziej. To nie jest kwestia naiwności, lecz emocji, które w sieci łatwo stają się narzędziem manipulacji.

Zespół Antyfraud posiada także system odpowiedzialny za bezpieczeństwo i na co dzień dba o jego rozwój, uwzględniając zmieniające się zagrożenia. – W dobie technologii to człowiek staje się najbardziej podatnym ogniwem, nie z powodu swojej słabości, ale z powodu

emocji, które mogą być przeciwko niemu wykorzystane – uśmiecha się Klaudia Olszak.
Ofiarami oszustw, takich jak na przystojnego oficera armii amerykańskiej czy nigeryjskiego księcia, najczęściej padają kobiety, choć trafiają się również mężczyźni, ale zdecydowanie rzadziej – co wynika z naszych obserwacji. Zdaniem Klaudii Olszak, najtrudniejszym zadaniem staje się uświadomienie poszkodowanym, że padły ofiarą oszustwa.

A jak reaguje na tego typu wyłudzenia AML?

Przede wszystkim należy wyjaśnić na czym polega proces przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Z punktu widzenia Anity Szyndlar, przeciwdziałanie praniu pieniędzy (w dużym skrócie) polega na niedopuszczeniu, aby środki finansowe pochodzące z nielegalnych źródeł trafiły do legalnego obrotu. Naszym głównym zadaniem jest weryfikacja źródła pochodzenia środków znajdujących się na rachunkach klientów i uzasadnić ich realizacje. W tym celu wykorzystujemy zaawansowane mechanizmy systemowe, które umożliwiają identyfikację i analizę transakcji zarówno w czasie rzeczywistym, jak i po ich dokonaniu. Nowoczesne rozwiązania technologiczne pozwalają nam badać coraz większą

Oszustwa finansowe mają różne oblicza - dlatego tak ważna jest współpraca zespołów AML i Fraud.

liczbę informacji, jednak nie zastępują roli analityka. To właśnie jego eksperckie doświadczenie nadaje procesowi dodatkową wartość – jest tą „wisienką na torcie", która decyduje o skuteczności całego procesu.
W obszarze AML nie zawsze mamy możliwość samodzielnego wykrywania wszystkich przypadków oszustw, dlatego zespoły ds. fraudów i AML ściśle współpracują, na bieżąco wymieniając informacje o zdarzeniach.
– Przykładem może być sytuacja tzw. „nigeryjskiego księcia". Po zidentyfikowaniu oszustwa przez zespół Fraud informacja trafia do naszego zespołu AML – wyjaśnia Anita Szyndlar.
Każde takie zgłoszenie rejestrowane jest jako podejrzane i analizowane w systemie pod kątem prania pieniędzy oraz finansowania terroryzmu przez eksperta AML. Kluczowe jest budowanie świadomości, że oszustwo fraudowe może stanowić tzw. oszustwo bazowe, które następnie może zostać wykorzystane do realizacji procesu prania pieniędzy.

Oszustwa w sieci. Jak nie dać się złapać?

Oszustwa finansowe mają różne oblicza - dlatego tak ważna jest współpraca zespołów AML i Fraud, które nie tylko analizują transakcje, ale także reagują na coraz bardziej wyrafinowane metody oszustów. A jednym z najczęściej wykorzystywanych kanałów jest właśnie internet.
Mimo licznych ostrzeżeń w mediach, wciąż poznajemy kolejne historie ofiar. Najczęściej ofiarami są osoby starsze, które nie posiadają komputera z dostępem do internetu, unikają portali społecznościowych i mogą być nieświadome aktualnych zagrożeń ale coraz częściej oszukiwani są także młodsi użytkownicy, którzy na co dzień korzystają z internetu – mówi Klaudia.

Współpraca to nie wszystko

Choć zespoły AML i Fraud łączą siły, aby reagować na zagrożenia, sama wymiana informacji nie wystarczy. Jak zauważają Klaudia i Anita, równie ważne jest systematyczne poszerzanie wiedzy – zarówno na podstawie kolejnych przypadków oszustw i wyłudzeń, jak i dzięki korzystaniu z różnych źródeł. Dopiero połączenie współpracy, wiedzy i świadomości pracowników oraz klientów pozwala skutecznie przeciwdziałać zagrożeniom.
Pracownicy zespołu antyfraud analizują każdy przypadek fraudowy i reagują na nowe metody oszustów. W przypadku AML kluczowe znaczenie ma natomiast znajomość schematów prania pieniędzy i umiejętność rozpoznawania jego etapów. Mówimy tu o podziale na: lokowanie środków, maskowanie i integrację. Każda z tych faz ma na celu ukrycie prawdziwego źródła pochodzenia pieniędzy – od momentu ich wprowadzenia do obiegu aż po zalegalizowanie, np. poprzez wpłatę na rachunek bankowy.

Edukacja jako narzędzie prewencji

Jak podkreślają ekspertki, równie ważna jak znajomość procedur jest edukacja – zarówno pracowników, jak i klientów. To właśnie świadomość zagrożeń pozwala szybciej rozpoznać nietypowe sytuacje i reagować na nie zanim dojdzie do strat. Regularne szkolenia, kampanie informacyjne czy proste komunikaty bezpieczeństwa sprawiają, że pracownicy potrafią lepiej identyfikować ryzyka, a klienci stają się bardziej odporni na manipulacje.
– Każdy świadomy klient to dodatkowa linia obrony przed oszustami. Im więcej osób wie, jak działają przestępcy, tym trudniej im osiągnąć cel – podsumowuje Anita.
Dlatego zostawiamy dla Was nasze High 5 dla bezpieczeństwa w sieci:

1. Nie klikaj w podejrzane linki. Zawsze sprawdzaj nadawcę wiadomości – czy to SMS, e-mail czy komunikator.
2. Nie daj się poganiać. Jeśli ktoś wywiera presję czasu, zatrzymaj się i zweryfikuj treść zanim zareagujesz.
3. Sprawdzaj źródło. Korzystaj tylko z oficjalnych kanałów kontaktu – to najpewniejsza droga.
4. Reaguj na próby oszustwa. Podejrzane wiadomości prześlij na numer 8080 – pomagasz wówczas chronić innych.
5. Chroń swoje konta. Aktualizuj system, używaj silnych haseł i włącz uwierzytelnianie dwuskładnikowe (2FA). ●

Współpraca Jerzy Sygidus

Kiedy cyberzagrożenie staje się katalizatorem zmian

Daniel Krzywiec
SGB-Bank

Początek 2024 roku przyniósł głośne ostrzeżenie dla całego sektora – atak ransomware na bank spółdzielczy. Złośliwe oprogramowanie zaszyfrowało dane, paraliżując funkcjonowanie banku i udowadniając, że nie ma instytucji zbyt małych, by być celem cyberataku. Każdy incydent jest dla nas lekcją, a ten kryzys stał się momentem, w którym przeszliśmy od reagowania do proaktywnego umacniania swojej pozycji lidera w obszarze cyberbezpieczeństwa.

W odpowiedzi na skalę zagrożenia, grupa SGB podjęła historyczną decyzję: Wdrożyliśmy największe w Polsce, zaawansowane, skonsolidowane rozwiązanie SOC w środowisku chmurowym dla wszystkich banków spółdzielczych! Skala bez precedensu – centralizacja bezpieczeństwa dla setek niezależnych banków spółdzielczych to najbardziej kompleksowe wyzwanie konsolidacyjne w Polsce – ujednoliciliśmy reguły obrony w niezwykle złożonym środowisku. Dzięki modelowi Cloud SOC, każdy bank spółdzielczy zyskuje ten sam, światowej klasy poziom ochrony, co największe banki w Polsce. Wyeliminowaliśmy koszty utrzymania sprzętu i uzyskaliśmy natychmiastową skalowalność – czyniąc obronę nieporównywalnie bardziej efektywną kosztowo, uzyskując maksymalną efektywność operacyjną. Każda anomalia wykryta w jednym banku spółdzielczym jest natychmiast analizowana przez centralny SOC, który uczy się i wzmacnia obronę sieci całej Grupy. Oznacza to, że klienci Banków Spółdzielczych SGB korzystają z ochrony na poziomie największych banków komercyjnych.

To więcej niż platforma cyberbezpieczeństwa – to jeden z najbardziej zaawansowanych kroków technologicznych w polskim sektorze finansowym.

Centrum dowodzenia SOC

W modelu zrzeszeniowym wdrożyliśmy jedną wspólną platformę cyberbezpieczeństwa, która wykorzystuje najnowocześniejszą technologię do analizowania wektorów ataków i wdrażania nowych reguł obrony, które chronią banki spółdzielcze. Eksperci SOC poszukują zagrożeń, opierając się na wiedzy o światowych trendach cyberataków. Ta wiedza jest natychmiast aplikowana do sprawdzenia w infrastrukturze banków spółdzielczych. Jeśli zidentyfikowane zostanie nowe zagrożenie w jednym z banków spółdzielczych, w ciągu kilku minut wdrażane są mechanizmy obronne w całej Grupie.

Współczesne cyberzagrożenia to nie pojedyncze przypadki, lecz zorganizowane działania prowadzone przez grupy przestępcze. Ataki są coraz bardziej wyrafinowane, wykorzystujące zaawansowane techniki, takie jak ransomware, ataki typu zero-day czy phishing. Dla pojedynczego banku spółdzielczego, utrzymanie zespołu ekspertów i infrastruktury zdolnej do ciągłego przeciwdziałania takiemu spektrum zagrożeń byłoby trudne do zrealizowania – SOC SGB jest odpowiedzią na te wyzwania i jednocześnie fundamentem cyfrowej transformacji całej Grupy.

Dzięki centralizacji SOC, grupa SGB zyskuje turbodoładowanie w wyścigu rynkowym. Klienci zyskują zaufanie i pewność, że lokalny bank spółdzielczy jest wsparty globalnym, technologicznym poziomem bezpieczeństwa. W rezultacie, SOC SGB to inwestycja, która przekształciła cyberbezpieczeństwo z kosztu w strategiczną przewagę konkurencyjną. Banki Spółdzielcze SGB mogą w pełni koncentrować się na swojej misji wspierania lokalnych społeczności, nie martwiąc się o skomplikowane i kosztowne wyzwania cyberbezpieczeństwa.

Nasza misja jest jasna: budowanie bezpiecznej bankowości przyszłości. Nasza dewiza jest prosta i niezmienna: #SILNI RAZEM! ●

Tam, gdzie klikamy, tam atakują

Jakub Borucki
Związek Banków Polskich

Cyberprzestępcy coraz częściej działają tam, gdzie spędzamy najwięcej czasu – w telefonie, poczcie elektronicznej, mediach społecznościowych czy na komunikatorach. Wykorzystują socjotechnikę, sztuczną inteligencję, presję czasu i nasze naturalne emocje. Najnowsze analizy branżowe pokazują, że próby oszustw rosną z roku na rok, a metody stają się coraz bardziej wyrafinowane. Dlatego dziś kluczową umiejętnością jest nie tylko korzystanie z bezpiecznych usług bankowych, ale także świadome poruszanie się w cyfrowym świecie.

Fałszywy doradca inwestycyjny, czyli presja, obietnice i... strata oszczędności

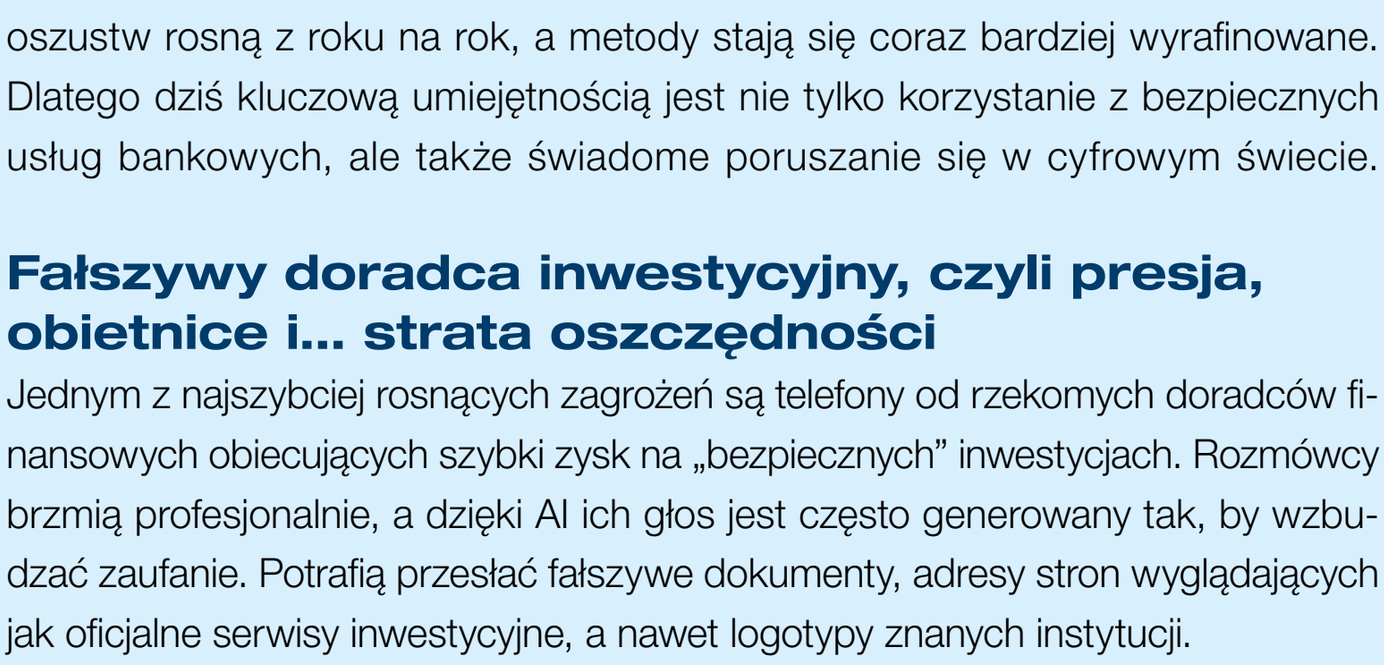
Jednym z najszybciej rosnących zagrożeń są telefony od rzekomych doradców finansowych obiecujących szybki zysk na „bezpiecznych” inwestycjach. Rozmówcy brzmią profesjonalnie, a dzięki AI ich głos jest często generowany tak, by wzbudzać zaufanie. Potrafią przesłać fałszywe dokumenty, adresy stron wyglądających jak oficjalne serwisy inwestycyjne, a nawet logotypy znanych instytucji.
Mechanizm jest zawsze podobny: oszust prosi o instalację dodatkowej aplikacji, która pozwala mu przejąć kontrolę nad urządzeniem lub nakłania do przekazania danych logowania. W efekcie traci się dostęp do środków, a czasem również do kont e-mail czy mediów społecznościowych. Najważniejsza zasada: żaden prawdziwy doradca nie gwarantuje zysków i nigdy nie prosi o zdalny dostęp do telefonu ani komputera.

Quishing, czyli pułapka ukryta w kodzie QR

Jeszcze niedawno kod QR kojarzył się przede wszystkim z wygodą: szybkim dostępem do menu, strony internetowej czy płatności. Dziś stał się również narzędziem oszustów. Fałszywe kody pojawiają się na plakatach, ulotkach, w SMS-ach, a coraz częściej także podczas sprzedaży internetowej. Po zeskanowaniu użytkownik trafia na stronę podszywającą się pod bank, sklep lub pośrednika płatności. Wygląda wiarygodnie, ale jej celem jest wyłudzenie loginów, haseł i danych kart.
Ofiary najczęściej mówią potem: „przecież to wyglądało normalnie”. I właśnie na tym polega skuteczność tego oszustwa – na wykorzystaniu naszego zaufania do technologii. Dlatego warto zapamiętać kilka zasad: skanuj wyłącznie te kody, które pochodzą z pewnych źródeł, nigdy nie loguj się po zeskanowaniu bez upewnienia się, gdzie faktycznie trafiłeś, a wszelkie niepewności traktuj tak, jak podejrzany e-mail czy podejrzany link.

Przejęcie konta na Facebooku i prośba o szybki BLIK

„Możesz mi wysłać kod BLIK? Oddam za 5 minut” – to jeden z najczęściej powtarzających się komunikatów wśród ofiar oszustw internetowych. Schemat zaczyna się niewinnie – znajomy wysyła wiadomość z prośbą o pomoc. Problem w tym, że zwykle… to nie jest znajomy, tylko ktoś, kto przejął jego konto. Atak rozpoczyna się od kliknięcia w fałszywy link (np. do rzekomego artykułu, zdjęcia lub konkursu), który prowadzi do strony podszywającej się pod Facebooka. Po wpisaniu hasła cyberprzestępcy natychmiast przejmują profil i w jego imieniu proszą o kody BLIK od kolejnych osób. Warto pamiętać, że bank nigdy nie pyta o kod BLIK, a prawdziwy znajomy zrozumie, jeśli oddzwonisz i upewnisz się, czy to na pewno on pisze. Dodatkowo włączenie dwuskładnikowego logowania znacząco ogranicza ryzyko przejęcia konta.



> W cyfrowym świecie nie trzeba być ekspertem, by być bezpiecznym – wystarczy być czujnym.

Cyberprzestępcy grają na emocjach i manipulują treściami, dlatego warto sprawdzać źródła, daty i opinie ekspertów.

Dziesięć codziennych nawyków, które naprawdę chronią

W cyberbezpieczeństwie nie chodzi o jednorazową decyzję, lecz o dobre nawyki, które wykonujemy automatycznie, tak jak zapinanie pasów w samochodzie. Dlatego, zamiast szukać „magicznej aplikacji", warto zacząć od najprostszych, codziennych zachowań, które realnie podnoszą nasze bezpieczeństwo.

1. Chroń swoje dane osobowe.
   Wielu z nas publikuje w sieci więcej, niż powinno – od zdjęcia z dowodem po celebrację zdanej teorii na prawo jazdy. A to skarbnica informacji dla przestępców, którzy na tej podstawie potrafią błyskawicznie zbudować profil ofiary.
2. Aktualizuj oprogramowanie i antywirusa.
   Nowe zagrożenia pojawiają się każdego dnia, a aktualizacje są jak wymiana zamków w drzwiach — bez nich trudno mówić o bezpieczeństwie.
3. Używaj silnych haseł i włącz 2FA.
   Długie, złożone i regularnie zmieniane — najlepiej zarządzane przez menedżer haseł. Dwuskładnikowe uwierzytelnienie to dodatkowa bariera, którą trudno przełamać.
4. Wylogowuj się po zakończonej pracy.
   To prosty odruch, który chroni Twoje konto przed przejęciem, zwłaszcza gdy korzystasz z urządzeń poza domem.
5. Korzystaj bezpiecznie z bankowości elektronicznej.
   Zawsze wpisuj adres banku ręcznie, sprawdzaj kłódkę przy adresie strony, wykonuj przelewy z zaufanych urządzeń. Pamiętaj — bank nigdy nie prosi o hasła ani kody PIN.
6. Unikaj podejrzanych stron i linków.
   Jeden nieostrożny klik może otworzyć cyberprzestępcom drogę do Twoich danych. Zawsze sprawdzaj certyfikat strony i dokładny adres URL.
7. Ostrożnie otwieraj wiadomości i załączniki.
   E-mail to ulubione narzędzie cyberprzestępców. Weryfikuj nadawcę, nie otwieraj załączników z nieznanych źródeł i sprawdzaj, dokąd prowadzi każdy link.
8. Twórz regularne kopie zapasowe.

Jeden nieostrożny klik może otworzyć cyberprzestępcom drogę do Twoich danych.

   Backup pozwala odzyskać ważne pliki po awarii sprzętu, kradzieży telefonu czy ataku ransomware.
9. Weryfikuj informacje, unikaj fake newsów.
   Cyberprzestępcy grają na emocjach i manipulują treściami, dlatego warto sprawdzać źródła, daty i opinie ekspertów – zwłaszcza przed udostępnianiem.
10. Edukuj się – codziennie.
    Banki i instytucje finansowe regularnie ostrzegają przed nowymi metodami oszustw. Kilka minut poświęconych na przeczytanie komunikatu może ochronić Twoje dane i pieniądze.

Dziesięć zasad, które właśnie poznałeś, nie wymagają specjalistycznej wiedzy ani kosztownych narzędzi. To codzienna, zdrowa cyfrowa rutyna, która daje realną ochronę.

Szczegółowe wskazówki, przykłady oraz materiały edukacyjne znajdziesz na stronie: www.dbamoswoje.pl ●

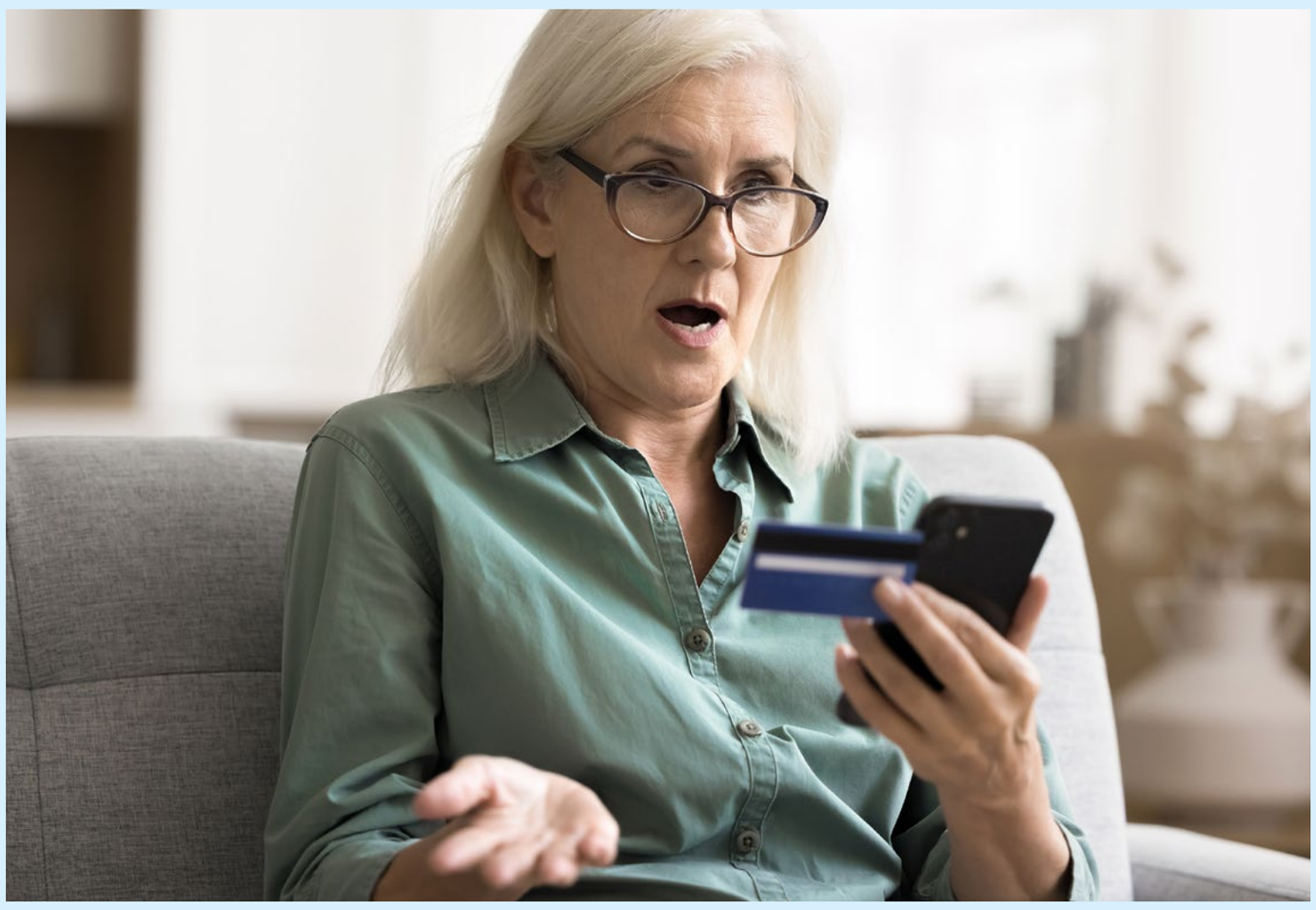
Fałszywa twarz, fałszywy głos i bardzo niepewna inwestycja

Robert Azembski

Cyberprzestępcy nie odpuszczają, chwytając się coraz bardziej podstępnych sposobów na oszukanie klientów banków spółdzielczych. W formie syntetycznej i w jednym miejscu, zebraliśmy najczęściej ostatnio stosowane metody oszustw. Teoretycznie sposobów na naciąganie klientów może być (i pewnie jest!) więcej, lecz niektóre powtarzają się z uporczywą regularnością. Co zatem mamy na tapecie? Oto rzut oka na stosowane oszustwa.

Fałszywy głos

Phishing – dziś w sieci na nieuważnych czeka wiele nowych domen-pułapek. Ale to nie wszystko. Przy tzw. voice phishing z wykorzystaniem AI, oszuści wysyłają do potencjalnych ofiar spersonalizowane e-maile albo dzwonią podszywając się pod bank, posługując się wygenerowanym przez AI fałszywym głosem pracownika banku. W ten sposób chcą wyłudzić dane logowania lub potwierdzenie przelewu. Co w takiej sytuacji robić?



„Średnia wartość transakcji oszukańczej wyniosła 1894,5 zł, co oznacza wzrost o 235,3 zł względem I kwartału 2025 r.” – czytamy w raporcie NBP.

- Klient banku powinien sam sprawdzić adres strony i kłódkę, a najlepiej samodzielnie i ręcznie wpisać adres witryny swojego banku.
- Klient ma także prawo poprosić pracownika o zidentyfikowanie się na swoim profilu (nie przez email czy sms!) internetowym w banku. Może także oddzwonić do banku, by osobiście upewnić się, czy wszystko jest „ok”. Bank zaś musi być przygotowany na takie sytuacje.

Fałszywa twarz

Deepfake (głos/wideo) – „szef”, ktoś „bliski” czy „zaufany”, prosi o szybki przelew lub kod blik. Przykładowo: w 2024 roku, w firmie Arup, doszło do oszustwa, gdy pracownik zaakceptował fałszywe polecenie przelewu na 25 mln dolarów tylko na podstawie wideokonferencji z dyrektorem finansowym i menedżerami. Wszyscy oni byli wygenerowani przy użyciu deepfake. Oszuści wykorzystują klony głosu i twarzy do podszywania się pod pracowników banków (w tym pod jego szefostwo!) albo pod budzących szczególne zaufanie klientów, co pozwala im np. telefonicznie nakłonić do wykonania przelewów.

- Warto zawsze zweryfikować taką sytuację innym kanałem komunikacji z bankiem i nie działać pod presją czasu.
- Nie należy klikać w linki z SMS/komunikatorów, ani na nie oddzwaniać, ale – jak już

wspomniałem – wchodzić na stronę banku ręcznie.
- Nigdy też nie podawać danych karty/hasła poza oficjalnym serwisem.
- Nie wolno instalować aplikacji z linków przesłanych od „kupujących”, czy „konsultantów”, ani udostępniać zdalnego sterowania pulpitem (AnyDesk/TeamViewer) osobom nieznajomym. W razie wątpliwości należy wykonać telefon do banku!

Wymuszenie, wyłudzenie, szantaż albo groźba

Ransomware z tzw. podwójnym wymuszeniem. Ataki bandziorów wymuszają nie tylko okup za odblokowanie danych, lecz także grożą ujawnieniem lub sprzedażą wrażliwych danych klientów banków, co dodatkowo wywiera presję na potencjalną ofiarę. Tu też radzimy skontaktować się osobiście z bankiem oraz z odpowiednimi służbami, które rozpoczną właściwe czynności śledcze.
Na OLX/Vinted + WhatsApp – w tym przypadku kupujący wysyła link do „odbioru pieniędzy” zaś wyłudzacz prosi o dane karty/BLIK lub instalację podesłanej aplikacji. Nie wolno się na to zgodzić. Płatności akceptować tylko w serwisie, w którym przeprowadzana jest transakcja.
Na SMS „na ZUS”/ prąd np. PGE/gaz z PGNiG/GSM – po groźbie odcięcia świadczeń/energii/telefonu podesłany zostaje link do „dopłaty” na fałszywą bramkę płatniczą. Rzecz należy zweryfikować w oficjalnej aplikacji operatora lub na osobistym koncie klienta.

Według danych NBP, w II kwartale 2025 r. odnotowano 104.073 transakcje oszukańcze, czyli o 6,1% mniej niż w poprzednim kwartale, jednak ich łączna wartość wzrosła o 7,2% – do 197,2 mln złotych.

Na email wysłany jakoby z „Profilu zaufanego” - przestępcy rozsyłają e-maile wyglądające jak wiadomości z Profilu Zaufanego. W ich treści informują, że zalogowano się z nowego urządzenia i podają numer telefonu kontaktowego. Zdezorientowany klient sam dzwoni pod wskazany numer i słyszy, że ktoś skradł jego dane na Profilu Zaufanym oraz że skontaktuje się z nim bank. W rzeczywistości to nie oddzwania bank, lecz podszywający się pod pracownika banku oszust, który nakłania do przelewów. Twierdzi, że ktoś próbował wykonać przelewy i że aby zabezpieczyć środki, klient musi przelać pieniądze na „konto techniczne”.
Jak się więc przed tym bronić?
- Przede wszystkim należy sprawdzić adres nadawczy (czasem drobna nawet różnica powinna wzbudzić już podejrzenia). Oczywiście nie oddzwaniać na numery z wiadomości.
- Także i w tym przypadku nie wolno działać w pospiechu i ulegać presji – oszuści często na to liczą!

Tak zwane „pewne inwestycje”

Reklamy z wizerunkami znanych osób, obietnice szybkiego zarobku, prośba o instalację „platformy”. To wszystko też są metody oszustów. Nie wolno wpłacać pieniędzy, ani nie udostępniać pulpitu! Niedawno rozbito grupę ▶

przestępczą odpowiedzialną za prowadzenie nielegalnych platform inwestycyjnych. Śledztwo, które objęło kilka platform finansowych ujawniło przestępcze działania, które doprowadziły do wyłudzenia około 75 mln zł od ponad 1500 osób. W wyniku zatrzymań i przeszukań zabezpieczono mienie na 5 mln zł, w tym kryptowaluty oraz dobra luksusowe – biżuterię i samochody. Ostatnio jednego z seniorów zamieszkałych w Nysie nabrano na takie fałszywe inwestycje. Inny mieszkaniec Nysy już nie dał się „wkręcić". Pomimo, że sprzedaż jakoby akcji zyskującego na wartości ORLENU była wsparta bardzo podobną do orlenowskiej stroną internetową oraz nawet nieźle spreparowanymi „dokumentami" towarzyszącymi fikcyjnej emisji walorów (m.in. podpisanym przez przewodniczącego KNF dr Stanisława Kluzę, który dawno już nie sprawuje tej funkcji! Naciskano także na szybki przelew zaliczki, by zarezerwować sobie zakup. Jak nie dać się „wkręcić" w tego rodzaju „atrakcyjne" inwestycje?

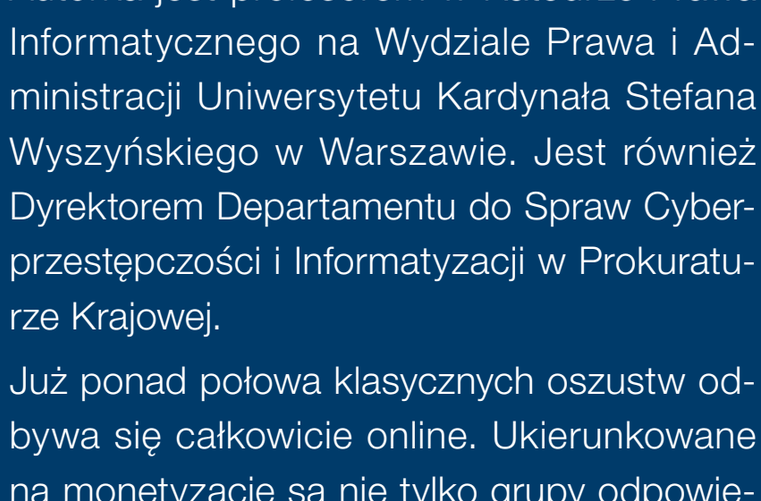
- Sprawdź w swoim banku, czy coś wiedzą o inwestycji, na którą jesteś namawiany, poproś, by się zorientowali w tej sprawie.
- Zadzwoń do dużego biura maklerskiego w dużym mieście i zapytaj o to samo.

Czujnym być i nie poddawać się presji

Nie ustają też napady na środki w bankomatach – złodzieje, tak jak już niegdyś bywało, montują na nich skanujące nakładki. Jedno włożenie karty i pieniądze mogą wyparować z konta. Trzeba być przenikliwym i zachować czujność!

- Klienci powinni zachować szczególną ostrożność, nie ufać komunikatom telefonicznym lub mailowym bez weryfikacji.
- Klienci powinni stosować silne zabezpieczenia kont (np. dwustopniową autoryzację) oraz zgłaszać wszelkie podejrzane sytuacje odpowiednim instytucjom.

Przed przestępcami ostrzegają i oczywiście zabezpieczają swoje systemy same banki. Ostrzeżenia i alerty wysyłają także policja i rożne instytucje publiczne. Ale także sam klient musi zadbać o swoje pieniądze. Bo to ludzie, to my jesteśmy sami bardzo często tym najsłabszym ogniwem, w które uderzają przestępcy, więc także ponosimy odpowiedzialność za naszą naiwność i błędy. ●



Prof. ucz. dr hab. inż. Agnieszka Gryszczyńska

Autorka jest profesorem w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Jest również Dyrektorem Departamentu do Spraw Cyberprzestępczości i Informatyzacji w Prokuraturze Krajowej.

Już ponad połowa klasycznych oszustw odbywa się całkowicie online. Ukierunkowane na monetyzację są nie tylko grupy odpowiedzialne za oszustwa w serwisach aukcyjnych i społecznościowych, fałszywe sklepy internetowe, oszustwa inwestycyjne, czy na tzw. legendę, love scam i ransomware, ale również oszuści tworzący strony podszywające się pod panele logowania do poczty elektronicznej, mediów społecznościowych, bankowości elektronicznej czy zajmujące się infekowaniem użytkowników internetu złośliwym oprogramowaniem.

W okresie okołoświątecznym ostrzegam także przed rosnącą ilością oszustw wykorzystujących fałszywe sklepy internetowe, oszustw na portalach aukcyjnych oraz ataków polegających na tym, że sprawcy podszywając się pod podmioty świadczące usługi kurierskie wysyłają wiadomości SMS z żądaniem dopłacenia do przesyłki i linki do fałszywych stron. Ich celem jest wyłudzenie danych dostępowych do bankowości elektronicznej.

Najważniejsze dla zachowania bezpieczeństwa jest czytanie ze zrozumieniem przychodzących wiadomości, weryfikowanie informacji oraz unikanie działania pod presją czasu lub emocji. Każda „superoferta" powinna również wzbudzić naszą czujność. Należy sprawdzać regulaminy i dane kontaktowe sklepów internetowych. Nie ulegać ofertom nadzwyczajnych inwestycji, a jeśli ktoś nas prosi o przesłanie kodu BLIK, warto skontaktować się z tą osobą innym kanałem komunikacji i to potwierdzić. Podejrzane wiadomości SMS przesyłajmy na numer 8080 do NASK na stronie incydent.cert.pl. Fałszywe strony internetowe można również zgłosić do mObywatela. Dzięki temu mogą zostać szybciej zablokowane, co ochroni również innych użytkowników internetu. Polecam również zastrzeganie numeru PESEL.

Damian Szulakowski
"Change" Enthusiast
ISSA Polska

Osoby prywatne dają się oszukać przede wszystkim przez manipulację emocjami – strach, chciwość, ciekawość i pośpiech, wyłączają logiczne myślenie. Cyberprzestępcy wykorzystują także przeładowanie informacyjne przestrzeni publicznej oraz brak wiedzy technologicznej, zwłaszcza u seniorów - w 2025 roku co dwudziesty senior był celem oszustów, tracąc średnio 40 tys. zł dziennie. W Polsce 31% osób doświadczyło prób wyłudzenia w sieci pieniędzy lub danych. Z kolei profesjonalni przedsiębiorcy padają ofiarą podobnych technik socjotechnicznych, czego konsekwencje bywają naprawdę dotkliwe. W 2025 roku 32% firm MŚP miało kontakt z oszustwami finansowymi, a 19,2% padło ofiarą ataków. Główne wektory ataków to phishing (94,7% incydentów) oraz ransomware. Średni koszt ataku wynosi 1,5-2,73 mln zł, a 60% małych firm bankrutuje po poważnym incydencie.

Osoby prywatne mogą się bronić przez weryfikację nadawcy, unikanie klikania podejrzanych linków, zastrzeżenie numeru PESEL, uwierzytelnianie dwuskładnikowe (2FA). Natomiast firmom można doradzić regularne szkolenia pracowników (77% ataków przy prowadzeniu odpowiedniej edukacji jest blokowanych), MFA, tworzenie kopi zapasowych oraz planów odzyskiwania danych.

Co haker wyczyta z Twojego selfie z biurka

Agnieszka Szelejewska
Head of content w takaoto.pro

Przyznaję się bez bicia: co roku, tuż przed świętami, oddaję się rytuałowi oglądania wszystkich części „Harry'ego Pottera". Tak, jestem Millenialsem. Tak, dorastałam z Potterem. I nie, nie wstydzę się tego ani trochę. W „Insygniach Śmierci" jest scena, która idealnie oddaje współczesne zagrożenia cybernetyczne. Harry, Ron i Hermiona ogłuszają przypadkowych pracowników Ministerstwa Magii, przybierają ich tożsamości za pomocą eliksiru wielosokowego i infiltrują jedno z najbardziej strzeżonych miejsc w magicznym świecie. A dzisiejszy haker? On nie potrzebuje różdżki. Potrzebuje Google'a, kilku darmowych narzędzi OSINT i Twojej nieuwagi podczas beztrosko wykonywanego selfie, by krok po kroku odsłaniać coraz więcej...

Polska liderem ataków ransomware

We wrześniu 2025 roku CERT Polska zarejestrował 26,4 tysiąca incydentów bezpieczeństwa – to wzrost o 278% w porównaniu z analogicznym miesiącem rok wcześniej[1]. Miesiąc później, w październiku 2025, liczba ta skoczyła do 40,1 tysiąca incydentów, co stanowi wzrost o 52%[2]. Ministerstwo Cyfryzacji wskazuje, że Polska znajduje się w pierwszej piątce najbardziej atakowanych krajów w Unii Europejskiej, a polskie firmy są celem ataków hakerskich ponad 250 razy dziennie. W pierwszej połowie 2025 roku Polska znalazła się nawet na pierwszym miejscu na świecie (!) pod względem liczby wykrytych ataków ransomware (złośliwego oprogramowania wymuszającego okup), odpowiadając za 6% wszystkich globalnych incydentów i wyprzedzając nawet Stany Zjednoczone. Haker nie potrzebuje magii. Potrzebuje Google'a, kilku darmowych narzędzi OSINT i Twojej nieostrożności.

1 https://cert.pl/uploads/docs/Podsumowanie_CSIRT_NASK_2025_09.pdf
2 https://cert.pl/uploads/docs/Podsumowanie_CSIRT_NASK_2025_10.pdf

OSINT, czyli gdy Google staje się narzędziem przestępcy

OSINT (Open Source Intelligence) to nic innego jak wywiad z otwartych źródeł. Polega na pozyskiwaniu i analizie informacji dostępnych publicznie – z mediów społecznościowych, raportów, zdjęć, filmów, baz danych czy nawet forów internetowych. To potężne narzędzie pomagające w wykrywaniu zagrożeń, analizie ryzyka, a także szybkiej reakcji na incydenty. Przykładowo banki wykorzystują OSINT do monitorowania aktywności w dark webie, gdzie pojawiają się wykradzione dane klientów, co pozwala na błyskawiczne zamknięcie luk bezpieczeństwa.

Specjaliści ds. bezpieczeństwa korzystają z OSINT, by śledzić kampanie phishingowe, identyfikować fałszywe profile i mapować sieci hakerów. Jego dobre oblicze ujawnia się także w ratowaniu życia. Dzięki analizie dostępnych publicznie danych, zdjęć czy filmów, służby potrafią szybciej lokalizować osoby zaginione, trafiając na tropy, które inaczej mogłyby przejść niezauważone. Bezpiecznie i legalnie przeszukuje ocean informacji, by przywrócić światłość tam, gdzie zapadła ciemność.

Ale OSINT – jak miecz obosieczny – może zarówno chronić, jak i ranić. To także potężne narzędzie w rękach cyberprzestępców i hakerów, którzy korzystają z tych samych mechanizmów, by przeprowadzać precyzyjne ataki socjotechniczne i mapować cele. Twoje selfie z biura, opublikowane bez refleksji, z widocznym badge'em czy monitorem w tle, staje się dla nich mapą drogową do wejścia do firmy lub przejęcia tożsamości. Zbierają kawałek po kawałku – od lokalizacji z metadanych, przez detale na karteczkach, po kontakty w social mediach – by w efekcie zbudować profil, który pozwoli na skuteczny atak. Dla hakera Twoje selfie to nie wspomnienie z pracy. To punkt startu śledztwa, które krok po kroku odsłoni, gdzie pracujesz, z kim, nad czym i kiedy jesteś najbardziej bezbronny.

Identyfikator: co zdradza Twój biurowy portret

Współczesne smartfony robią zdjęcia o takiej rozdzielczości, że nawet rozmazany w tle badge można powiększyć i odczytać z niego: imię i nazwisko pracownika, stanowisko i dział, kod kreskowy lub QR, który często służy jako klucz dostępu, format loginu (np. imie.nazwisko@bank.pl).

Dysponując tymi danymi, przestępca może zlecić wykonanie fałszywego identyfikatora i spróbować wejść do budynku – to tzw. tailgating, gdy „nowy pracownik" podąża za kimś przez drzwi wymagające autoryzacji.

Haker nie potrzebuje magii. Potrzebuje Google'a, kilku darmowych narzędzi OSINT i Twojej nieostrożności.

Haker, znając z badge'a imię, nazwisko i stanowisko, może przygotować spersonalizowanego maila, SMS lub zadzwonić, podszywając się pod IT lub dział HR, by nakłaniać do podania haseł albo kliknięcia w zainfekowany link. Dane z identyfikatora często wystarczają, by uwiarygodnić wiadomość („dzień dobry, jestem z działu bezpieczeństwa – widzę, że pracuje pan/pani w dziale X…"). Na tej podstawie potrafi pozyskiwać kolejne dane – np. znaleźć adres zamieszkania, PESEL lub inne szczegóły w ogólnodostępnych rejestrach, a następnie wykorzystać je do kradzieży tożsamości lub zaciągania kredytów „na słupa". Identyfikator bywa punktem wyjścia do analizy struktury firmy (kto gdzie pracuje, jak wyglądają e-maile, jakich systemów używa się w danej organizacji), co pozwala prowadzić dalsze ataki na większą skalę. Ale badge to dopiero początek…

EXIF i metadane – cyfrowe odciski palców Twojego zdjęcia

Większość użytkowników smartfonów nawet nie zdaje sobie sprawy, że każde wykonane zdjęcie niesie ze sobą niewidzialne dane, zwane EXIF (Exchangeable Image File Format). To takie cyfrowe odciski palców, które oprócz samego obrazu zawierają dodatkowe informacje techniczne i kontekstowe. Mamy tam m.in. dokładną datę i godzinę wykonania zdjęcia, model telefonu czy aparatu, wersję systemu operacyjnego. Przy zrzutach ekranu smartfon lub komputer zostawia ślad użytkownika – może to być na przykład nazwa konta na komputerze.

Szczególnie istotne dla bezpieczeństwa są dane geolokalizacyjne, czyli współrzędne GPS. Kiedy aktywujesz geolokalizację w aparacie telefonu, każde zrobione zdjęcie zapisuje dokładne miejsce, gdzie zostało wykonane – czasem z precyzją do kilku metrów. Kiedy dodajesz do internetu zwykłe selfie z biurkiem w tle, dla Ciebie to miła pamiątka, a dla hakera – mapa z dokładnym adresem, który może wykorzystać do zaplanowania fizycznego wejścia do Twojej firmy, śledzenia Twoich codziennych zwyczajów, analizowania wzorców pracy zespołu itd.

Na szczęście narzędzia do odczytywania i usuwania EXIF są dostępne publicznie – na przykład darmowy ExifTool pozwala nie tylko na odczyt wszystkich metadanych, ale i ich modyfikację bądź usunięcie. Możesz też wyłączyć zapisywanie lokalizacji GPS w zdjęciach na smartfonie: wystarczy w ustawieniach aparatu wyłączyć opcję geotagowania (na iPhonie znajdziesz to w „Prywatność" -> „Usługi lokalizacji" -> „Aparat", a na Androidzie „Aparat" -> Ustawienia aparatu (ikona koła zębatego) -> Lokalizacja, Zapisywanie lokalizacji lub Geotagowanie (nazwa może się różnić w zależności od modelu).

Dla hakera Twoje selfie to nie wspomnienie z pracy. To punkt startu śledztwa, które krok po kroku odsłoni, gdzie pracujesz, z kim, nad czym i kiedy jesteś najbardziej bezbronny.

Karteczki, odbicia, notatki: jak haker czyta między wierszami

Haker nie ogranicza się do tego, co jest widoczne na pierwszy rzut oka. Czyta „między wierszami" – analizuje odbicia, cienie, rozmyte tła. Analitycy OSINT potrafią zidentyfikować lokalizację na podstawie odbicia w okularach, oku czy szkle. Odbicie może ujawnić, co jest wyświetlane na monitorze, kto stoi obok, a nawet jaki jest układ pomieszczeń biurowych.

Ludzie wciąż przyklejają hasła do monitorów i na tablice. Wszelkie karteczki samoprzylepne z zapisanymi kodami dostępu, numerami telefonów do działów IT, a nawet hasłami do

kont służbowych mogą być z łatwością odczytane i wykorzystanie w niecnych celach. Podobnie jak fragmenty dokumentu, listy klientów i umowy NDA leżące na blacie. Haker powiększy zdjęcie, zastosuje filtr wyostrzający i odczyta interesującą go informację. Nieostry fragment okna z systemem bankowym, adres e-mail klienta w otwartej skrzynce, nazwa aplikacji – wszystko to może zostać wydobyte przy użyciu publicznie dostępnych narzędzi OCR (przekształcających obrazy w edytowalny tekst). Nawet schemat sieci z adresami IP.

Ba! Możliwe jest nawet odczytanie tła dźwiękowego. Jeśli publikujesz krótkie wideo z biura, analitycy OSINT potrafią ustalić lokalizację na podstawie dźwięków w tle – natężenia ruchu ulicznego, echa w pomieszczeniu, charakterystycznych odgłosów. Haker nie czyta tylko tego, co pokazujesz. Czyta odbicia w Twoich okularach, karteczki za monitorem i echo w nagraniu. Czyta wszystko.

Prywatność w zagrożeniu: jak selfie z biura wpływa na Twoje życie prywatne

Selfie z biura to nie tylko zagrożenie dla firmy. To także zaproszenie dla przestępców do Twojego życia prywatnego. Wieści o tym, że „nareszcie odpoczywamy w naszej wymarzonej willi na Mazurach" albo „Toskania naszym letnim azylem" to dla włamywaczy jasny komunikat: dom pusty, czas działać. Połączenie takich zdjęć z informacjami o codziennych zwyczajach czy miejscach pracy pozwala stworzyć dokładny profil całej rodziny – gdzie są, kiedy wrócą i co mają w domu. Wyobraź sobie rodziców, którzy chwalą się zdjęciem dziecka bujającego się na huśtawce i dopisują hasztagi typu #ulubionyplaczabaw czy komentarze opisujące dokładne miejsce. Dla przestępców to klarowny znak z napisem „tu przebywa potencjalna ofiara". Połączenie tych szczegółów pozwala określić adres zamieszkania, przedszkole czy szkołę, ulubione alejki w parku czy godziny pobytu w domach. To wszystko tworzy dokładny profil, który może zostać wykorzystany do ataków socjotechnicznych, włamań, porwań czy stalkingu.Dlatego zawsze warto pamiętać o wyłączaniu geotagów, ograniczaniu publicznego udostępniania lokalizacji i nie spieszyć się z publikacją zdjęć np. z urlopu, bo bezpieczeństwo zaczyna się od tej pierwszej chwili, gdy post trafia do sieci.

Jak się wystrzegać: dobre praktyki OSINT i ochrona prywatności

Ochrona przed OSINT nie wymaga magii – wystarczy świadomość i konsekwencja:

1. Usuń metadane EXIF przed publikacją: korzystaj z narzędzi typu EXIFCleaner lub aplikacji mobilnych, które automatycznie czyszczą dane GPS i techniczne.
2. Sprawdź tło przed wrzuceniem zdjęcia: badge, monitor, karteczki, dokumenty – upewnij się, że w kadrze nie widać żadnych danych wrażliwych.
3. Wyłącz geolokalizację w aparacie: to najprostsza i najskuteczniejsza obrona przed ujawnieniem lokalizacji.
4. Nie publikuj na żywo: oznaczaj lokalizację dopiero po opuszczeniu miejsca.
5. Dbaj o higienę cyfrową: stosuj silne hasła, świadome zarządzanie ustawieniami prywatności w mediach społecznościowych.
6. Przeszkol zespół – np. poprzez uczestniczenie w warsztatach OSINT. Jasno określ zasady, co można, a czego nie można publikować, oraz regularnie przeprowadzaj audyty.

W erze cyfrowej każde selfie to dowód rzeczowy. Pytanie brzmi: czy chcesz, by został użyty przeciwko Tobie?

A wracając do uniwersum Harrego Pottera… Ministerstwo Magii zostało zinfiltrowane przez trójkę, która miała eliksir i plan. Twoje biuro może być zinfiltrowane przez hakera, który ma tylko Twoje selfie z poranną kawą – z badge'em na szyi, na tle tablicy z hasłami. Ale w przeciwieństwie do eliksiru, Twoje zdjęcie nie traci mocy po godzinie. Zostaje w sieci na zawsze i może być wykorzystywane wielokrotnie, bez ograniczeń czasowych. Więc zanim klikniesz „Opublikuj", zadaj sobie pytanie: co widzę na tym zdjęciu? A co zobaczy haker? Bo może się okazać, że Twoje beztroskie selfie to dla przestępcy dokładnie to, czym dla Harry'ego był eliksir wielosokowy – przepustka do miejsca, gdzie być nie powinien. W cyberbezpieczeństwie nie ma drugiej szansy na pierwsze wrażenie. Raz opublikowane zdjęcie pozostaje w sieci na zawsze. ●

Haker nie czyta tylko tego, co pokazujesz. Czyta odbicia w Twoich okularach, karteczki za monitorem i echo w nagraniu. Czyta wszystko.

Co zrobić, gdy zgubisz telefon - praktyczny poradnik

Krzysztof Swoboda
Technical content manager w takaoto.pro

Smartfon jest dzisiaj portfelem, kluczem do banku i pamiętnikiem w jednym – jego utrata często oznacza nie tylko koszt zakupu nowego urządzenia, ale realne ryzyko kradzieży tożsamości i środków finansowych. Z policyjnych i branżowych danych wynika, że telefony pozostają jednymi z najczęściej kradzionych przedmiotów. Na szczęście dobra wiadomość jest taka, że większość negatywnych konsekwencji takiego zdarzenia można zminimalizować, jeśli wcześniej zadba się o kilka kluczowych ustawień i procedur.

Dlaczego zgubiony telefon jest groźniejszy, niż się wydaje

Istnieją ogromne szanse na to, że Twój smartfon przechowuje znacznie więcej niż listę kontaktów – zawiera dostęp do bankowości mobilnej, poczty, chmury z dokumentami oraz kanałów autoryzacji płatności i logowania. Telefon stał się centralnym „tokenem dostępowym" do usług cyfrowych, co sprawia, że jego fizyczna utrata jest równie niebezpieczna jak wyciek haseł.

Policja i media branżowe wskazują, że w Polsce co roku zgłaszanych jest niemal dziesięć tysięcy kradzieży telefonów komórkowych[1]. Jednocześnie dane z rynków europejskich pokazują, że w największych miastach liczba kradzieży smartfonów rośnie, a urządzenia są systematycznie wykorzystywane do przejmowania kont bankowych i portfeli cyfrowych – a to oznacza, że zachowanie czujności to już nie opcja, a wręcz obowiązek!

> Pod żadnym pozorem nie przechowuj haseł i kodów PIN do bankowości w notatkach, galeriach zdjęć czy komunikatorach.

Z perspektywy banku i klienta najpoważniejsze ryzyko nie wynika z samej wartości smartfona, ale z możliwości przejęcia SMS-ów autoryzacyjnych, aplikacji mobilnej, komunikatorów i skrzynki mailowej. W swoim raporcie CSIRT KNF zwraca uwagę, że oszuści coraz częściej łączą kradzież lub przejęcie telefonu z socjotechniką, podszywając się pod bank lub instytucje publiczne, by wyłudzić dodatkowe kody i dane logowania[2]. Widać więc tutaj niepokojący trend – obecnie złodzieje grają o wiele wyższą stawkę, za którą należałoby uznać oszczędności całego Twojego życia.

Jak się chronić? Postaw na mocną blokadę ekranu i włącz szyfrowanie

Podstawowym zabezpieczeniem jest silna blokada ekranu – najlepiej w postaci długiego kodu PIN (minimum 6 cyfr) lub hasła alfanumerycznego, wspieranego przez biometrię w postaci odcisku palca lub rozpoznawania twarzy. Zarówno ENISA, jak i krajowe poradniki cyberbezpieczeństwa, w tym CERT Polska, zalecają unikanie prostych wzorów czy PIN-ów typu „1234" czy czterech lub sześciu takich samych cyfr, na przykład: 0000.

Uwierzytelnianie biometryczne łączy wygodę użytkowania z wysokim poziomem ochrony. Co istotne, większość współczesnych urządzeń przechowuje dane biometryczne lokalnie, nie przesyłając ich do chmury, co eliminuje ryzyko ich przejęcia przez osoby trzecie.

Kolejnym kluczowym elementem jest wyłączenie podglądu powiadomień na zablokowanym ekranie. Treść wiadomości SMS z kodami bankowymi lub powiadomienia z aplikacji mogą być widoczne nawet bez odblokowania telefonu, co pozwala przestępcy uzyskać dostęp do kodów autoryzacyjnych bez znajomości hasła.

W systemie Android wejdź w:

- Ustawienia -> Powiadomienia -> Na ekranie blokady i wybierz opcję „Ukryj wrażliwe treści".

1 https://testy-do-policji.pl/jakie-masz-szanse-na-odzyskanie-skradzionego-telefonu-przez-policje-fakty
2 https://www.knf.gov.pl/knf/pl/komponenty/img/Raport_roczny_CSIRT_KNF_88762.pdf

W iOS wystarczy wejść w:

- Ustawienia -> Powiadomienia -> Pokaż podgląd i ustawić „Nigdy" lub „Gdy odblokowane".

Współczesne smartfony domyślnie szyfrują pamięć urządzenia, ale pełna ochrona działa tylko wtedy, gdy blokada ekranu jest faktycznie używana i automatycznie się aktywuje po krótkim okresie bezczynności – nie dłuższym niż 30 sekund. Warto również wyłączyć automatyczne łączenie z otwartymi sieciami Wi-Fi i regularnie pobierać aktualizacje systemu operacyjnego oraz aplikacji – to sposób na ograniczenie ryzyka wykorzystania znanych luk bezpieczeństwa, który nie wymaga od Ciebie podejmowania praktycznie żadnych długotrwałych działań, na które w ciągu dnia nie zawsze miałbyś czas.

Uwierzytelnianie biometryczne łączy wygodę użytkowania z wysokim poziomem ochrony. Co istotne, większość współczesnych urządzeń przechowuje dane biometryczne lokalnie, nie przesyłając ich do chmury, co eliminuje ryzyko ich przejęcia przez osoby trzecie.

Aktywuj zdalne zarządzanie i twórz kopie zapasowe

Producenci systemów mobilnych oferują wbudowane usługi lokalizacji i zdalnego zarządzania urządzeniem, takie jak „Znajdź" (Find My iPhone) czy „Znajdź moje urządzenie" w Androidzie.

Umożliwiają one namierzenie telefonu na mapie, odtworzenie głośnego dźwięku, szybkie zablokowanie ekranu wraz z komunikatem dla znalazcy, a nawet zdalne wymazanie danych. UKE w swoim poradniku wprost wskazuje te funkcje jako jedno z najważniejszych narzędzi obrony w razie zgubienia lub kradzieży smartfona.

W przypadku Androida należy przejść do menu:

- Ustawienia -> Google -> Znajdź moje urządzenie i włączyć tę opcję, upewniając się jednocześnie, że lokalizacja jest aktywna.

W iOS wystarczy wejść w:

- Ustawienia -> [Twoje imię] -> Znajdź -> Znajdź mój iPhone i włączyć tę funkcję wraz z opcjami „Sieć Znajdź" i „Ostatnia lokalizacja".

To zabezpieczenie działa nawet wtedy, gdy telefon jest offline – w przypadku iOS wykorzystywana jest wówczas sieć innych urządzeń Apple w trybie szyfrowanego przekazywania sygnału.

Równie ważne jest regularne tworzenie kopii zapasowych, które obejmują zwłaszcza:

- kontakty,
- kalendarz,
- zdjęcia,
- dokumenty,
- ustawienia aplikacji,
- historię wiadomości.

Każdy użytkownik Androida ma dostęp do Dysku Google z domyślnie 15 GB przestrzeni[3], podczas gdy właściciele iPhone'ów mogą korzystać z iCloud oferującego 5 GB w wersji bezpłatnej. Wiele smartfonów wykonuje backup automatycznie, zapisując zmiany na bieżąco, dzięki czemu użytkownik ma dostęp do najbardziej aktualnej wersji swoich danych.

Oprócz rozwiązań producentów warto rozważyć zdywersyfikowanie miejsc przechowywania backupu poprzez korzystanie z uniwersalnych usług chmurowych, takich jak Dropbox czy OneDrive. Nawet jeśli jedno konto zostanie przejęte, dane będą dostępne z innego źródła.

Wzmocnij bezpieczeństwo bankowości mobilnej

Dla przestępcy najcenniejszą częścią przejętego telefonu nie jest „urządzenie samo w sobie", ale aplikacje bankowe, portfele cyfrowe i mechanizmy płatności zbliżeniowych.

Pod żadnym pozorem nie przechowuj haseł i kodów PIN do bankowości w notatkach, galeriach zdjęć czy komunikatorach, nawet jeśli są „zaszyfrowane" pozornie nieoczywistym opisem.

O wiele lepszym rozwiązaniem jest wykorzystanie menedżera haseł (np. Dashlane, 1Password, Keeper), który bezpiecznie przechowuje wszystkie dane logowania w zaszyfrowanej formie, wymagając zapamiętania jedynie hasła nadrzędnego.

Najlepsze rozwiązania wykorzystują architekturę zero-knowledge oraz 256-bitowe szyfrowanie AES, co oznacza, że dane są szyfrowane na poziomie urządzenia użytkownika, a dostawca usługi nie ma dostępu do kluczy deszyfrujących[4].

Pamiętaj też, by włączyć uwierzytelnianie wieloskładnikowe (multi-factor authentication, MFA), łączące coś, co wiemy (hasło), z czymś, co mamy (urządzenie), i czymś, czym jesteśmy (biometria). Według raportu Microsoft, zastosowanie 2FA eliminuje aż 99,9% zautomatyzowanych ataków na konta użytkowników[5].

Dobrym nawykiem jest także ograniczenie limitów transakcji mobilnych oraz włączenie powiadomień push lub SMS o każdej operacji na rachunku – to pozwala szybciej wychwycić nieautoryzowaną aktywność.

3 https://www.siberoloji.com/top-15-free-cloud-storage-services-available-in-2024/
4 https://www.keepersecurity.com/blog/2025/05/23/which-password-manager-is-the-most-secure/
5 https://www.welivesecurity.com/2020/03/09/microsoft-99-percent-hacked-accounts-lacked-mfa/

Stosuj zasadę minimalizacji danych

Każde zainstalowane na telefonie oprogramowanie jest potencjalnym „kanałem" dostępu do naszych informacji. Eksperci zalecają weryfikację uprawnień – szczególnie dostępu do lokalizacji, kontaktów, mikrofonu i aparatu – oraz rozważne logowanie przez konta społecznościowe. W systemie Android należy regularnie sprawdzać podmenu:

- Ustawienia -> Aplikacje ->[wybrana aplikacja] -> Uprawnienia i usuwać niepotrzebne uprawnienia.

W iOS:

- Ustawienia -> Prywatność, kontrolując, które aplikacje mają dostęp do lokalizacji, zdjęć i kontaktów.

Duża część złośliwego oprogramowania na telefony trafia na urządzenia przez aplikacje spoza oficjalnych sklepów lub z podejrzanych reklam i stron. Instalowanie programów tylko z zaufanych repozytoriów, jak Google Play czy App Store, jest jednym z prostszych, a zarazem najskuteczniejszych środków profilaktycznych.

W przypadku utraty telefonu nie zwlekaj z reakcją!

Jeśli zorientujesz się, że telefon został skradziony lub nie możesz go odnaleźć, kluczowe są pierwsze minuty – tak jak w klasycznym „incident response plan", który funkcjonuje w cyberbezpieczeństwie korporacyjnym.

Pierwszym krokiem powinno być zdalne zlokalizowanie i zablokowanie urządzenia przez konto producenta. Użytkownicy Androida powinni zalogować się na google.com/android/find z innego urządzenia, wybrać zgubiony telefon i zablokować go (wyświetli się komunikat dla znalazcy) lub wymazać dane urządzenia. Właściciele iPhone'ów powinni zalogować się na icloud.com/find, wybrać zgubione urządzenie i aktywować Tryb zaginięcia (Lost Mode) lub Wymaż iPhone. Równolegle należy skontaktować się z operatorem telefonicznym w celu zablokowania karty SIM, co uniemożliwi wykorzystanie numeru do potwierdzania transakcji i przejęcia komunikacji SMS.

Instytucje finansowe rekomendują też jak najszybszy kontakt z bankiem – najlepiej przez infolinię lub bankowość internetową z innego zaufanego urządzenia – w celu zablokowania dostępu mobilnego oraz ewentualnych instrumentów płatniczych.

Jak Spółdzielcza Grupa Bankowa chroni swoich klientów?

Banki Spółdzielcze SGB konsekwentnie inwestują w bezpieczeństwo cyfrowe na wielu poziomach, oferując kompleksową ochronę przed współczesnymi zagrożeniami. Wdrożony system monitorowania transakcji kartowych FDS (Fraud Detection System) zautomatyzował cały proces obsługi alertów[6].

Rozwiązanie przygotowane przez Zespół Cyberbezpieczeństwa SGB-Banku działa w oparciu o weryfikację kartowego profilu transakcyjnego klienta i wykrywanie anomalii, natychmiastowo informując o podejrzanych transakcjach oraz podejmując działania typu odmowa autoryzacji lub zablokowanie karty.

Centrum Operacji Bezpieczeństwa (SOC) SGB wykorzystuje nowoczesne technologie, procedury bezpieczeństwa oraz pracę specjalistów odpowiedzialnych za szybkie wykrywanie i analizę zagrożeń. Do podstawowego zakresu obowiązków SOC należy analiza i korelacja zdarzeń bezpieczeństwa, dostarczanie wskaźników IoC (Indicator of Compromise) dla istotnych zagrożeń sektorowych, monitoring i ochrona ruchu sieciowego, Web Filtering oraz detekcja złośliwego kodu.

SGB wdrożyło też platformę wykrywania i reagowania na zdarzenia sieciowe opartą na sztucznej inteligencji, która prowadzi analizę ruchu sieciowego i identyfikuje zagrożenia w czasie rzeczywistym.

Od marca 2024 roku SGB zmniejszyło maksymalną liczbę urządzeń, na których aplikacja mobilna SGB Mobile może być aktywowana, z 5 do 2[7]. To zabezpieczenie znacząco zmniejsza ryzyko nieautoryzowanego dostępu do bankowości mobilnej w przypadku kradzieży lub przejęcia telefonu czy tabletu.

Równocześnie Spółdzielcza Grupa Bankowa prowadzi systematyczne kampanie edukacyjne, publikując komunikaty o aktualnych zagrożeniach na stronie www.sgb.pl, ostrzegając klientów przed technikami oszustów, takimi jak spoofing numeru telefonu, phishing czy oszustwa wykorzystujące deepfake i sztuczną inteligencję.

Utrata smartfona to – owszem – spory problem, ale nie musi oznaczać katastrofy. Wdrożenie wyżej opisanych działań zajmie Ci zaledwie kilkanaście minut – to bardzo mało, jak na potencjalne korzyści, na czele z ochroną Twoich finansów i danych wrażliwych.

Zawsze pamiętaj jeszcze o jednej kwestii: bezpieczeństwo zaczyna się od Ciebie – od prostych, codziennych nawyków. Nawet najlepsza aplikacja, antywirus czy weryfikacja dwuetapowa nie uchroni Twoich danych, jeśli nie wykażesz się czujnością i… trzeźwą oceną sytuacji. ●

6 https://www.sgb.pl/fds-w-sgb-usluga-monitorowania-kart-w-bankach-spoldzielczych-sgb/
7 https://www.sgb.pl/zmiany-w-aktywacji-sgb-mobile/

Ataki na bankomaty – przestępcy, nakładki i kradzieże z kont klientów

Andrzej Borowiak
Rzecznik prasowy Komendanta Wojewódzkiego Policji w Poznaniu

Aż 500 milionów złotych w ubiegłym roku stracili Polacy w wyniku różnych oszustw, wyłudzeń, czy też kradzieży pieniędzy z kont. Te formy przestępczości stają się dominujące. Prześledźmy jeden z takich sposobów.

W Polsce wciąż pojawiają się doniesienia o przestępcach, którzy okradają klientów banków, wykorzystując zmodyfikowane bankomaty. Chodzi o nakładki montowane na czytniki kart, klawiatury czy wylot gotówki, a także ukryte kamery. Takie działania potocznie bywają nazywane z angielska „spofingiem", ale poprawne określenie, gdy mówimy o nakładkach na bankomaty i kopiowaniu kart, to skimming – od angielskiego to skim, czyli „zbierać"/„zgrywać" dane. W ostatnich latach w Polsce odnotowano szereg spraw, w których klienci tracili pieniądze po wypłatach z bankomatu. Niektóre z nich to klasyczne przykłady skimmingu z wykorzystaniem nakładek, inne – wariacje na ten temat, jak np. nakładki zatrzymujące wypłacone banknoty. Do tego dochodzą coraz sprytniejsze metody łączenia skimmingu z innymi formami oszustw.

Innym elementem jest fałszywa klawiatura lub nakładka na klawiaturę (PIN pad). To cienka, idealnie dopasowana nakładka, którą umieszcza się na oryginalnej klawiaturze bankomatu. Rejestruje ona wprowadzane klawisze – czyli PIN – i zapisuje lub przesyła go dalej. Alternatywnie przestępcy stosują ukrytą kamerę, np. w listwie nad klawiaturą, w ramce ekranu, w obudowie bankomatu albo nawet w plastikowym „kieszonkowym" daszku. Kamera jest skierowana na palce użytkownika.

Nakładki na bankomaty – czy to skimmery kopiujące dane z kart, fałszywe klawiatury rejestrujące PIN, czy elementy zatrzymujące fizycznie banknoty – pozostają realnym zagrożeniem dla klientów banków w Polsce.

Poniżej wyjaśniam, jak działają takie przestępstwa, i przedstawiam przykłady z Polski z ostatnich lat, a na końcu – praktyczne wskazówki, jak zminimalizować ryzyko.

Skimming bankomatowy to metoda kradzieży

polegająca na nielegalnym skopiowaniu danych z paska magnetycznego lub chipa karty płatniczej podczas korzystania z bankomatu, terminala czy innego urządzenia. Przestępcy montują w tym celu specjalne urządzenia – skimmery – bezpośrednio na bankomacie.
Najczęściej wykorzystywane elementy to nakładka na szczelinę, na kartę. Wygląda jak normalna część bankomatu, ale w środku znajduje się miniaturowy czytnik. Gdy klient wkłada kartę, urządzenie odczytuje dane z paska magnetycznego, a bankomat – tak jak zawsze – również rozpoczyna transakcję. Z punktu widzenia użytkownika wszystko wygląda normalnie.

Wykorzystywany jest również Moduł komunikacyjny lub pamięć. Zebrane dane z karty i PIN mogą być zapisane w pamięci urządze-

nia, które przestępcy później demontują. Mogą też być przesyłane na bieżąco np. przez Bluetooth czy sieć komórkową do innego urządzenia.
Mając dane z paska magnetycznego oraz PIN, przestępcy wytwarzają tzw. duplikaty kart i próbują wypłacać pieniądze z bankomatów – zwykle poza Polską. Wynika to z tego, że bankomaty w Polsce od lat wymagają transakcji w trybie chip & PIN, więc samo sklonowanie paska nie wystarcza. Polskie karty można jednak bez problemu sklonować paskiem i wykorzystać np. w urządzeniach za granicą, gdzie wciąż zdarzają się mniej restrykcyjne ustawienia. Robią to też u nas w kraju przez podstawione osoby.
Wariantem tej metody są nakładki, które fizycznie zatrzymują banknoty w momencie wypłaty – klient widzi komunikat, że transakcja przebiegła pomyślnie, ale nie dostaje gotówki i często odchodzi zdezorientowany. Przestępcy demontują później nakładkę i zabierają uwięzione pieniądze.
Jesienią 2025 r. w Polsce wybuchła jedna z największych afer związanych z nieuprawnionymi wypłatami z bankomatów. Z kont 490 klientów Santander Bank Polska zniknęło łącznie ok. 2,2 mln zł. Prokuratura Okręgowa w Bydgoszczy wszczęła zbiorcze śledztwo, wskazując, że mamy do czynienia z działalnością zorganizowanej grupy przestępczej. Bank potwierdził, że doszło do nieautoryzowanych wypłat w różnych miejscach kraju. Klientom pieniądze mają zostać zwrócone, a karty – wymienione na nowe.
Co ważne, z perspektywy nakładek na bankomaty, policja i eksperci bardzo szybko skierowali podejrzenia w stronę skimmingu. Analizy wskazują, że prawdopodobnie przestępcy użyli specjalnych nakładek na bankomaty, które kopiowały dane z kart. Media donosiły, że pierwsze zgłoszenia pojawiły się m.in. w Poznaniu, a policjanci wytypowali co najmniej dwa bankomaty jako potencjalnie zmodyfikowane. W momencie oględzin urządzenia skanujące mogły już zostać jednak zdemontowane.
Sprawa z Poznania i Bydgoszczy pokazuje dwie kluczowe rzeczy: Metoda skimmingu z nakładkami na bankomaty jest nadal realnym zagrożeniem, mimo wprowadzanych przez banki zabezpieczeń. Skala strat może być ogromna, a ofiarami padają zarówno osoby korzystające z wypłat gotówkowych na co dzień, jak i klienci wypłacający gotówkę sporadycznie.

Jak się chronić przed nakładkami na bankomatach?

Żaden poradnik nie da 100% gwarancji bezpieczeństwa, ale stosując kilka prostych zasad, radykalnie zmniejszasz ryzyko, że padniesz ofiarą skimmingu.
Obejrzyj bankomat zanim go użyjesz. Zanim włożysz kartę zwróć uwagę na szczelinę na kartę – czy nie wygląda na „doklejoną”, czy nie jest luźna albo porysowana inaczej niż reszta obudowy. Sprawdź klawiaturę – czy nie wystaje podejrzanie, czy wszystkie przyciski wciskają się równo. Spójrz na górną część bankomatu – czy nie ma tam podejrzanych „listew”, plastikowych maskownic, elementów z dziwną dziurką, bo może to być kamera. Jeśli coś wygląda nietypowo – nie korzystaj z bankomatu i zgłoś sprawę do banku lub na policję.
Zawsze zasłaniaj PIN. To jedna z najważniejszych, a wciąż lekceważonych zasad. Zakrywaj klawiaturę całą dłonią lub portfelem podczas wprowadzania PIN. Nie wpisuj PIN-u, gdy ktoś stoi tuż za Tobą lub nadmiernie się przygląda. W miarę możliwości wybieraj bankomaty w dobrze oświetlonych, monitorowanych miejscach (oddziały banków, galerie handlowe) Nawet jeśli przestępcy skopiują dane z paska/chipa, brak PIN-u mocno ogranicza ich możliwości.
Monitoruj swoje konto i ustaw limity. Większość banków umożliwia ustawienie limitów dziennych dla wypłat i płatności kartą. Uruchom włączenie powiadomień push/SMS o każdej transakcji. Dobre też jest natychmiastowe zablokowanie karty w aplikacji mobilnej. Wykorzystując niski limit wypłat gotówki zmniejszasz potencjalne straty. Gdy zauważysz szybkie powiadomienie o wypłacie, której nie dokonałeś, pozwoli Ci to natychmiast zareagować.

W ostatnich latach w Polsce odnotowano szereg spraw, w których klienci tracili pieniądze po wypłatach z bankomatu.

Reaguj od razu na każdy niepokojący sygnał. Jeżeli bankomat „połknął” kartę, nie wydał gotówki mimo komunikatu o sukcesie, w historii widzisz wypłatę z miejsca, w którym nie byłeś, to natychmiast musisz coś zrobić. Zadzwoń na infolinię banku albo użyj aplikacji, by zastrzec kartę. Zgłoś reklamację i poproś o blokadę podejrzanych transakcji. Rozważ zgłoszenie sprawy na policję. Najlepiej to zrobić z wydrukiem historii transakcji lub zrzutami ekranu.
W sytuacjach takich jak sprawa Santandera z jesieni 2025 r. banki z reguły zwracają utracone środki, ale im szybciej zgłosisz problem, tym łatwiej udowodnisz, że to nie Ty wypłacałeś pieniądze.
Nakładki na bankomaty – czy to skimmery kopiujące dane z kart, fałszywe klawiatury rejestrujące PIN, czy elementy zatrzymujące fizycznie banknoty – pozostają realnym zagrożeniem dla klientów banków w Polsce. Sprawy takie jak fala nieuprawnionych wypłat z kont klientów Santandera w 2025 r. pokazują, że mimo rozwoju zabezpieczeń, przestępcy potrafią wykorzystywać luki systemowe i różnice w standardach bezpieczeństwa w różnych krajach.
Dobra wiadomość jest taka, że użytkownik ma realny wpływ na swoje bezpieczeństwo. Wystarczy kilka konsekwentnych nawyków. Dokładne oglądanie bankomatu przed użyciem, zasłanianie PIN-u, ustawienie sensownych limitów i powiadomień, no i szybka reakcja na każdy niepokojący sygnał. ●

Coraz większa świadomość zagrożeń

Janusz Orłowski

Warszawski Instytut Bankowości przedstawił najnowsze badanie zatytułowane „Postawy Polaków wobec cyberbezpieczeństwa 2025". Z raportu wynika, że najbardziej obawiamy się zagrożenia jakim jest w cyfrowym świecie phishing. Za kolejne, znaczące niebezpieczeństwa, badani respondenci uznali atak na cyfrową tożsamość oraz zjawisko dezinformacji i fake newsów.

Phishing, to przede wszystkim niebezpieczeństwo wyłudzenia danych osobowych i kodów dostępu i tym samym pieniędzy. Wielu badanych uważa atak na wirtualną tożsamość za bardzo niebezpieczną, jak również, że zjawisko dezinformacji jest groźne. Warto też zauważyć, że blisko co trzeci badany obawia się ataków hakerów na instytucje publiczne oraz zagrożeń związanych z instalowaniem złośliwego oprogramowania. Respondenci zwracają także uwagę na zagrożenia dotyczące mowy nienawiści i naruszania cudzej godności osobistej. Wielu badanych dostrzega również zagrożenia związane z oszustwami z wykorzystaniem sztucznej inteligencji.

Badani, którzy doświadczyli oszustwa osobiście albo ktoś bliski z ich otoczenia, deklarują, że najczęściej mają styczność z hakowaniem kont w mediach społecznościowych. Ofiary phishingu zwracają uwagę na niebezpieczeństwo oszustw telefonicznych, takich jak podszywanie się pod numery telefonów różnych instytucji, banków, urzędów, a nawet znanej osoby.

Warto zaznaczyć, że oszustw inwestycyjnych, za pośrednictwem rozmów telefonicznych z fałszywym doradcą, najczęściej doświadczają osoby w wieku od 35 do 44 lat, a poprzez fałszywe reklamy intratnej i szybkiej inwestycji, najmłodsi badani w wieku od 18 do 24 lat.

> Phishing pozostaje królem cyfrowych oszustw – wciąż łapiemy się na ten sam haczyk.

Niestety, mniej niż połowa Polaków twierdzi, że sprawdza wiarygodność informacji w przestrzeni cyfrowej, a zaledwie kilkanaście procent z nich weryfikuje je kilkoma różnymi metodami. Blisko połowa badanych przyznaje, że robi to nieregularnie i w zależności od źródła. Najczęściej czujność związaną z weryfikowaniem informacji i ich źródeł deklarują osoby z wykształceniem wyższym.

Ponad połowa badanych deklaruje, że potrafi rozpoznać fałszywe nagrania i zdjęcia stworzone przez sztuczną inteligencję, które mogą m.in. służyć do rozprzestrzeniania dezinformacji. Zdolność do weryfikacji takich fałszywek dominuje wśród osób w wieku 35 – 44 lata z wykształceniem wyższym.
Z badania wynika, że jeszcze rok temu było więcej przeciwników, niż zwolenników sztucznej inteligencji ale w tym roku tendencja ta się odwróciła. Dwukrotnie

Phishing, fałszywe inwestycje i dezinformacja – to największe cyfrowe lęki Polaków.

więcej Polaków widzi w sztucznej inteligencji szansę, a nie zagrożenie. Jednocześnie jednak badani starają się nie lekceważyć niebezpieczeństwa związanego z niewłaściwym zastosowaniem tej nowej technologii, ponieważ połowa badanych uważa, że sztuczna inteligencja ma zarówno zalety, jak i wady.
Mimo, że Polacy nadal najchętniej stosują kod PIN jako zabezpieczenie dostępu do telefonu komórkowego lub smartfona, to ostatnie badanie pokazało, że tyle samo respondentów odblokowuje te urządzenia za pomocą technologii biometrycznych, zarówno odciskiem palca, jak i skanem twarzy. Technologie biometryczne najczęściej wykorzystują młodzi dorośli w wieku 18 – 24 lata.
Ponad połowa badanych deklaruje, że ma aktualne oprogramowania antywirusowe na swoim smartfonie i komputerze. Ale jednocześnie co trzecia osoba aktualizuje antywirusa od czasu do czasu. Młodzi dorośli wolą bardziej zabezpieczyć swój telefon niż komputer, natomiast o zabezpieczenie komputera dbają bardziej seniorzy, pobierając aktualizację programu zawsze kiedy jest to wymagane.
Z badania wynika, że Polacy zbyt rzadko weryfikują telefonującą osobę, która przedstawia się jako pracownik banku, przez co narażają się na oszustwa, które grożą wyłudzeniem danych potrzebnych do zhakowania elektronicznego konta bankowego. Niespełna jedna trzecia respondentów sprawdza tożsamość takiej osoby telefonując samodzielnie do placówki bankowej.
Podejrzewając, że oszust zdobył dane, które umożliwiają mu, na przykład wyłudzenie pieniędzy albo zalogowanie się do bankowości internetowej lub mobilnej, większość bo 57% badanych od razu blokuje kartę płatniczą lub (55%) informuje telefonicznie swój bank

Blisko jedna trzecia badanych deklaruje dobrą znajomość zasad bezpieczeństwa w przestrzeni cyfrowej.

w celu wyjaśnienie wydarzenia i ewentualnej blokady konta. Ale zaledwie co trzecia badana osoba zdecydowałaby się na powiadomienie CERT Polska, czyli instytucji, która przyjmuje zgłoszenia phishingu.
Blisko jedna trzecia badanych deklaruje dobrą znajomość zasad bezpieczeństwa w przestrzeni cyfrowej, czyli więcej niż było to podczas zeszłorocznego badania. Mimo to prawie połowa respondentów posiada wciąż tylko orientacyjną wiedzę na ten temat. To pokazuje, że potrzebne są nadal działania edukacyjne, które będą podnosić wiedzę i umiejętności społeczeństwa w tym zakresie.
Prawie czterech na dziesięciu badanych wskazuje, że za bezpieczeństwo elektronicznych usług finansowych odpowiadają przede wszystkim banki. Część respondentów (29%) twierdzi, że finansowa ochrona powinna płynąć z różnych źródeł jednocześnie – od państwa, operatorów komórkowych i internetowych, producentów urządzeń czy firm rozliczających transakcje.
Instytucje bankowe przestają być więc traktowane jako jedyna tarcza ochronna elektronicznych finansów. Bardziej wyedukowane społeczeństwo zaczyna coraz częściej dostrzegać także swój wpływ na cyberbezpieczeństwo. Już blisko dwie trzecie badanych respondentów czuje się bezpiecznie w cyfrowym świecie, a coraz mniej osób odczuwa niepewność w tym zakresie, co może wskazywać na wyższy poziom świadomości zagrożeń. ●

Kiedy zaufanie **staje się pułapką**

Rozmowa z **Jackiem Walkiewiczem**, psychologiem, mówcą motywacyjnym, mentorem, o manipulacji, nawykach i bezpieczeństwie.

Jak pan, jako psycholog, rozumie zjawisko manipulacji w sieci? Czy współczesny człowiek jest na nią bardziej podatny niż kiedyś?

Zjawiska o których pan mówi są dla nas nowe, musimy się nauczyć, przyjąć do powszechnej wiadomości. Są trudne do wykrycia, ponieważ ci, którzy je przygotowują z nadzieją na ogromne zyski, precyzyjnie dopracowują wszystkie metody manipulacji. Myślę, że pierwszym powodem, dla którego one działają, jesteśmy my sami, bo zwykle reagujemy automatycznie, w sposób mocno nawykowy. Jeżeli ktoś dzwoni do nas i oznajmia, że telefonuje z banku, to my automatycznie zakładamy, że on rzeczywiście dzwoni z banku. Myślę, że moje pokolenie, a także pokolenie moich rodziców, jest szczególnie narażone na tę manipulację, bo dla nas osoba z urzędu czy banku była od zawsze osobą godną zaufania i nikt jej nigdy nie weryfikował, nie dopuszczał myśli, że ona wcale nie musi być pracownikiem banku i że na dodatek ma złe zamiary.

Myślę, że musimy się nauczyć poddawać krytyce wszystko, co może stanowić dla nas zagrożenie. Lepiej dmuchać na zimne i nie działać automatycznie, choć nie jest to takie łatwe. Sam zauważyłem, że kiedy ktoś prosi mnie o podanie jakiejś informacji, to ja mu ją podaję. Ta informacja na początku może być niewinna i prosta. Może dotyczyć na przykład czy w ostatnim miesiącu dokonałem jakiejś transakcji bankowej. W odpowiedzi piszę „tak”, później drugi raz piszę „tak” i kolejny „tak” – i wpadam w pewien automatyzm. Już przestaję myśleć, czy te udzielane informacje są dla mnie dobre, czy złe. Wniosek stąd jest

FOT. JACEKWALKIEWICZ.PL

prosty: praktyczne myślenie w przypadku instytucji, które są wrażliwe, typu banki i urzędy, powinno nam się włączać zawsze.

Powiedział pan, że to kwestia nawykowego myślenia. Czy jesteśmy w stanie się przed tym automatyzmem bronić?

Należy niewątpliwie zawsze włączać własną weryfikację, czyli kierować się zdrowym rozsądkiem, własną wiedzą i zawsze mieć ograniczone zaufanie w tych przypadkach, kiedy chodzi o wrażliwe informacje. W takich kwestiach powinniśmy mieć zawsze podejście krytyczne.

Od lat obserwujemy te same schematy oszustw – „na wnuczka”, „na policjanta”, „na pracownika banku” – mimo że media regularnie nagłaśniają przypadki osób, które w ten sposób tracą oszczędności całego życia. Z perspektywy praktyka: dlaczego, mimo tak szerokiej świadomości i ostrzeżeń, te metody wciąż działają na tak wielu ludzi?”

Tak jak już powiedziałem, wszyscy działamy automatycznie. Jeżeli ktoś nam mówi: „Dzień dobry, dzwonię z banku, czy w ostatnim tygodniu robił pan jakiś przelew?”, to się zaczynamy zastanawiać czy robiliśmy jakiś przelew, a nie nad tym, czy osoba dzwoniąca do nas chce nam ukraść pieniądze.

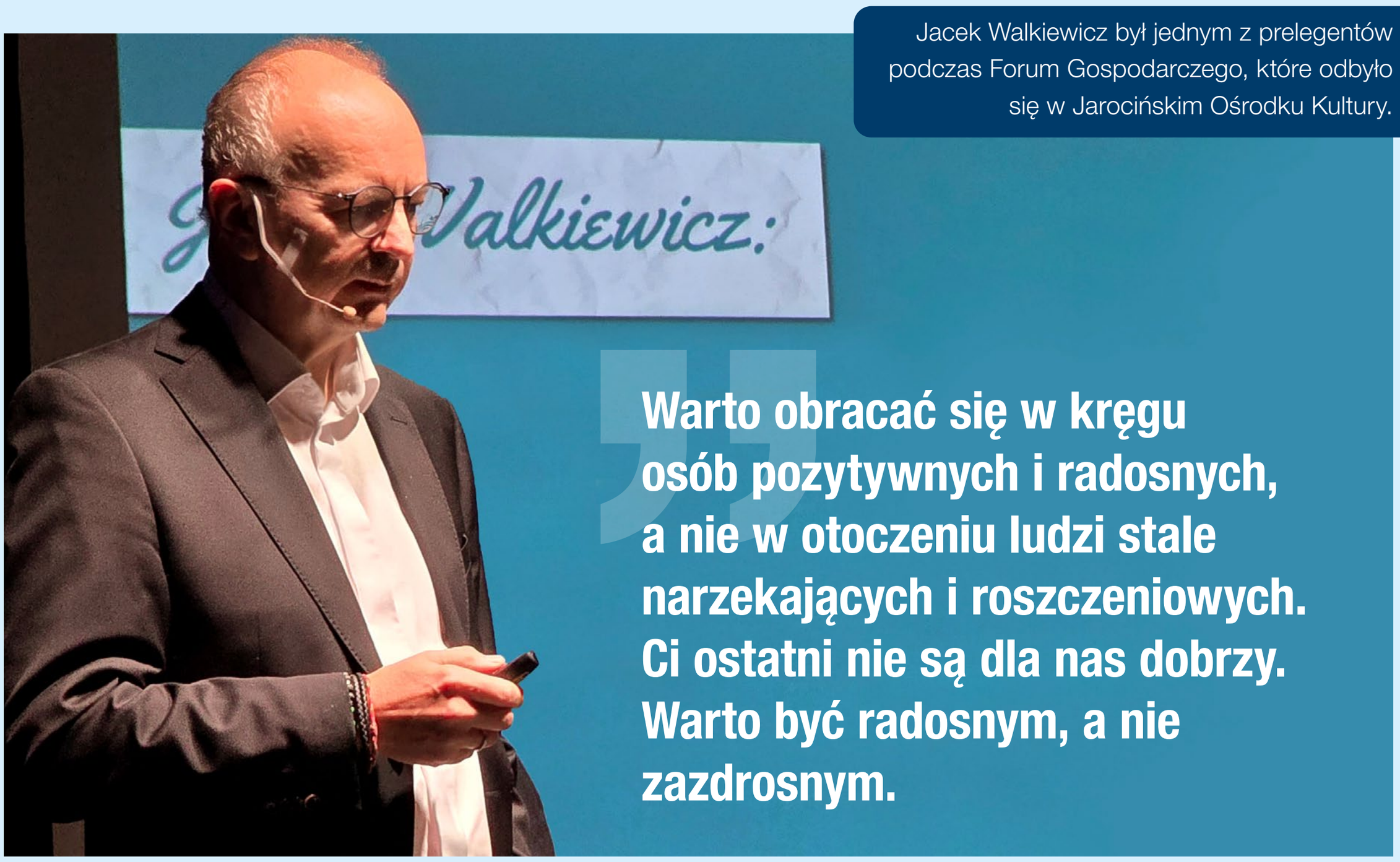
> Musimy się nauczyć poddawać krytyce wszystko, co może stanowić dla nas zagrożenie. Lepiej dmuchać na zimne i nie działać automatycznie, choć nie jest to takie łatwe.

Gdy chodzi zatem o zdalne podanie danych wrażliwych, najlepiej jest włączyć krytyczne myślenie i po prostu się rozłączyć. Zadzwonić do banku z pytaniem, czy oni rzeczywiście czegoś od nas chcą. To jednak wymaga krytycznego myślenia, a my jakże często zdajemy się na rozmaite zewnętrze wsparcia. Przykładowo – słuchając nawigacji, która prowadzi nas za kółkiem. Często, ku własnemu zaskoczeniu, nawigator każe nam skręcić w prawo i my skręcamy w prawo, lądując w konsekwencji na piaszczystej, polnej drodze. Nie pomyśleliśmy, że ta droga nie była dla nas najlepsza, że trzeba było pojechać główną szosą. Nie schodzimy z tych swoich „ścieżek myślenia”, ponieważ się nie zastanawiamy, czy ta droga jest dla nas dobra, czy zła. To jest właśnie ta umiejętność, której trzeba się nam nauczyć, aby być krytycznym w stosunku do odbieranych informacji. W ogóle, aby być krytycznym.

Czyli umiejętność krytycznego myślenia jest dzisiaj kluczowa.

Dokładnie tak. Konieczne jest uczciwe spojrzenie na naszą sytuację, czy ona jest dla nas bezpieczna. Ktoś dzwoni z banku i już z samego założenia jest to dla nas moment podwyższonego ryzyka, tak samo jak, gdy ktoś zadzwoni i powie, że dzwoni z policji i oznajmia, że jesteśmy przedmiotem zainteresowania przestępców. To przecież nie zdarza się na co dzień! W takich sytuacjach doradzam, aby mieć mniej zaufania do ludzi, których nie znamy, nie widzimy, a jedynie słyszymy w słuchawce telefonu.

Zdecydowanie powinniśmy mieć więcej uważności w tym, co robimy gdy rzecz dotyczy naszych pieniędzy czy innych naszych ważnych spraw. Myślę, że każdy może być ofiarą, ja również, bo to jest kwestia chwili, momentu, nastroju, przebiegłości, umiejętności wzbudzenia zaufania przez złych ludzi. Pamiętam, jak do moich rodziców zadzwonił ktoś i mama zapytała: Jasiu?, bo nie rozpoznała głosu. A ten ktoś odpowiedział: tak, Jasiu. Pierwsze, co zrobiła moja mama, to przekazała imię wnuka. I to imię powtarzane potem przez tę osobę uwiarygodniało ją. Moja mama nieświadomie przekazała tę informację. Powtarzam, bardzo łatwo jest nieświadomie powiedzieć coś, co przestępcy skrzętnie wykorzystają.



Jacek Walkiewicz był jednym z prelegentów podczas Forum Gospodarczego, które odbyło się w Jarocińskim Ośrodku Kultury.

FOT. ROMAN SZEWCZYK

Moja mam zachowałaby się dokładnie tak samo.

Myślę, że w stu procentach nie da się wszystkich ludzi nauczyć tej uważności i chłodnego krytycyzmu. Dlatego, po pierwsze, trzeba o tym dużo mówić w przestrzeni publicznej. Ale tak, jak pan wspomniał, mówi się o tym w telewizji, w mediach, a ludzie nadal dają się łapać na automatyczne myślenie. Ja uważam, że w takich sytuacjach najlepiej jest się rozłączyć. Jeżeli ktoś naprawdę dzwoni z banku, to zadzwoni po raz drugi. Natomiast jeżeli ktoś jest oszustem, to pewnie wybiera telefon z jakiegoś algorytmu, z jakiejś bazy i więcej nie zadzwoni. Lepiej więc od razu przyjąć założenie, że ten telefon obarczony był dużym ryzykiem oszustwa. Banki zresztą często same informują klientów, na swych stronach internetowych, czego nigdy nie żądają i o co nigdy nie będą pytały klientów. Czyli należy z góry przyjąć założenie, że mogę być ofiarą manipulacji i próby oszustwa. Jeżeli nie, to cudownie. A jeśli tak, to udało mi się obronić swoje zasoby i siebie. Dla pokolenia naszych rodziców taka reakcja bywa trudna, bo to jest pokolenie, które szanowało instytucje państwowe i banki. I z takiego wysokiego poziomu zaufania nagle trzeba im teraz zejść.

Jak rozwijać w sobie tę rozwagę, tę samoświadomość, by nie dać się zmanipulować przez te cudze narracje?

Przede wszystkim trzeba zacząć się urealniać i zobaczyć, co już mamy, a czego się boimy. Bo ludzie bardzo często nie doceniają tego, co mają. Wydaje im się, że ich życie jest nudne, kiepskie, bez sukcesów, a jak się ich spytamy, co osiągnęli, to okazuje się, że niczego nie widzą i nie doceniają. Ludzie po prostu nie doceniają swoich osiągnięć. Skończenie szkoły, zdanie matury, ukończenie studiów jest jakimś osiągnięciem. Powodem do bycia człowiekiem sukcesu. Ten sukces, taki naprawdę spektakularny, przychodzi czasami po wielu latach, albo w ogóle nie przychodzi. Albo dostępują go jedynie nieliczni. Mówiąc o sukcesie spektakularnym, mam na myśli kogoś, kto nagle został milionerem albo jest znany z jakiejś wyjątkowej pasji, jak choćby Robert Kubica. To są wyjątkowe osoby na 38 milionów rodaków.

Ale należy też zauważać swoje osobiste sukcesy, typu: może nie mamy wielkiego domu, ale mamy ten, który sami wybudowaliśmy. Może nie jesteśmy na pierwszych stronach gazet, ale robimy coś ważnego dla innych ludzi. Prowadzimy np. biznes, który jest ważny dla lokalnej społeczności. Pewnie, że jak wejdziemy na fora mediów społecznościowych i zobaczymy tam kogoś, kto zamieszcza foto czy video z Karaibów, gdzie pływa katamaranem, to nam się wyda, że to jest dopiero piękne życie. A nasze jest nudne. Ale przecież często potem dowiadujemy się, że ten bogacz z Karaibów, z jakichś bliżej nieznanych powodów, popadł w długi, depresję i zdesperowany popełnił samobójstwo. Ja to nazywam urealnianiem się, czyli zobaczeniem siebie w realnym świecie.

Mówi pan więc, by doceniać to, co mamy?

Doceniać i być wdzięcznym. Mam gdzie mieszkać, mam co jeść, mamy zdrowe dzieci, żyjących rodziców… Czego mi jeszcze trzeba? Bo prawda o nas jest taka, że jak się nie ucieszymy małym mieszkankiem, to duży dom też nas nie zadowoli. Co ważne, należy się obracać w kręgu osób pozytywnych i radosnych, a nie w otoczeniu ludzi stale narzekających i roszczeniowych. Ci ostatni nie są dla nas dobrzy. Warto być radosnym, a nie zazdrosnym.

Nie ma radości bez życzliwości. Często pan to mówi.

– Życzliwość, wspieranie się, dbanie o siebie... Wspieramy innych – to oznacza również, że wspieramy siebie. Bo kiedy pomagamy pokonywać trudności innym, to sami uczymy się czegoś nowego. Kto przewiezie innego człowieka na drugi brzeg, sam też tam dopływa.

Przed nami nowy rok. Czego życzyłby pan nam wszystkim w nadchodzącym 2026 roku?

– Rok 2026 może być rokiem przełomowym w sprawach geopolitycznych i być może naszych narodowych, a także i w osobistych sprawach wielu osób. Ci ostatni mogą stanąć przed zbyt licznymi opcjami i koniecznością właściwego wyboru. Życzyłbym wszystkim,

Zdecydowanie powinniśmy mieć więcej uważności w tym, co robimy gdy rzecz dotyczy naszych pieniędzy czy innych naszych ważnych spraw.

aby w obliczu tej zmienności, a być może w chaosie, kierowali się radą Wojciecha Młynarskiego „róbmy swoje”. Na trudne momenty, na trudne czasy, dobrze się jest trzymać swojego kursu życiowego. Dobrze jest wiedzieć, gdzie zmierzamy i co chcemy zrobić w życiu.

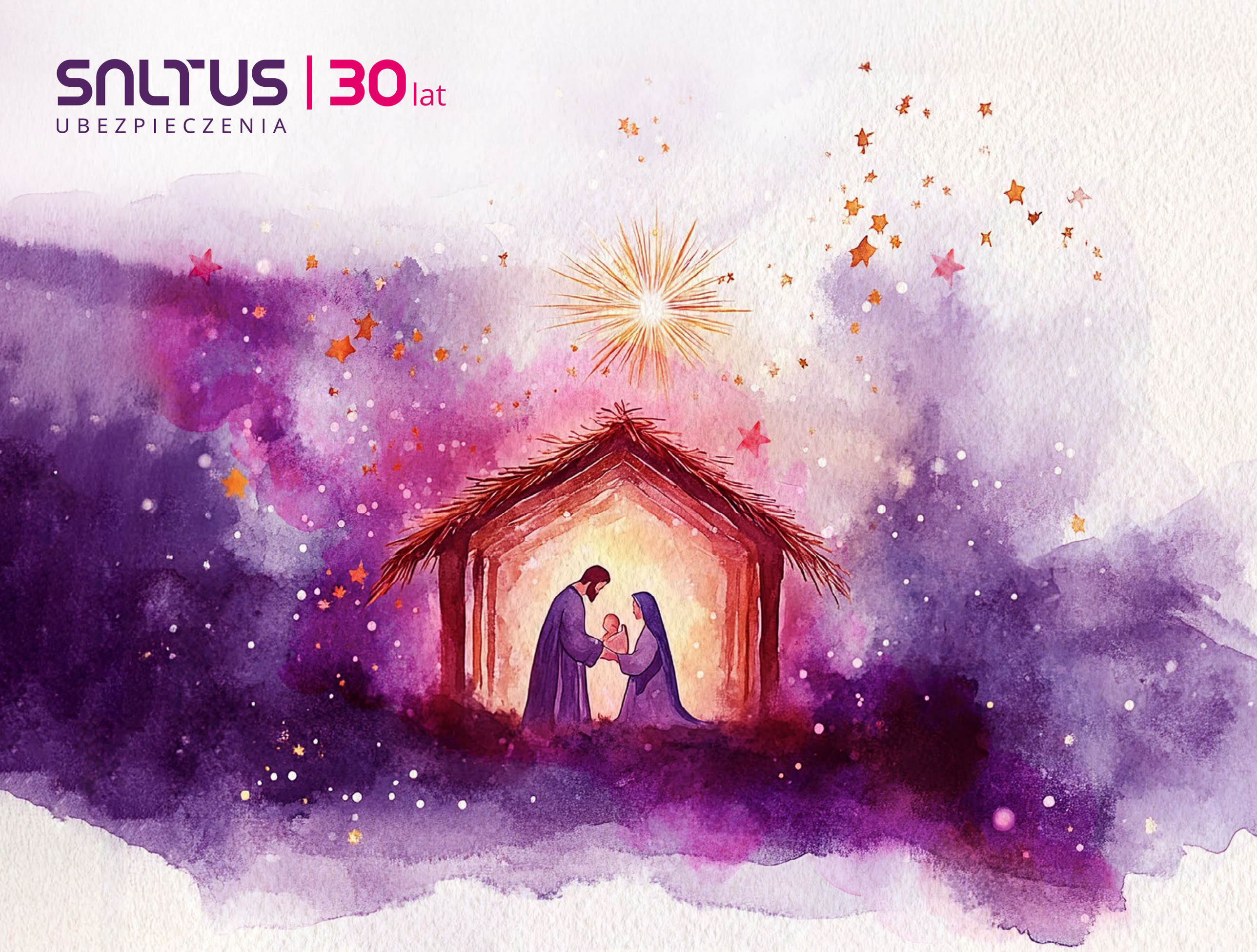
Życzyłbym wszystkim, by mieli poczucie, że są we właściwym czasie, we właściwym miejscu, z właściwymi ludźmi i robią właściwe rzeczy. Ażeby doznali poczucia głębokiego sensu swojego życia. Bo, myślę, że to jest coś, co w nadmiarze możliwości może gdzieś ludziom umykać. Zadać sobie pytanie: Czy to, co robię ma sens? Wszystkim życzę, aby mieli poczucie, że ich życie jest piękne.

Reasumując, niezależnie od tego, co się dzieje, co się działo i co może się dziać, to na zmartwienia najlepszy jest zawsze drugi człowiek, więc dbajmy o relacje z bliskimi, z dziećmi, ze swoimi rodzicami, z klientami, z przyjaciółmi i z obcymi ludźmi, których spotykamy na ulicy. Myślę, że to jest niezależne od czasu, historii, od naszego wieku, jest uniwersalne - bycie życzliwym dla siebie nawzajem, nie ma bowiem radości bez życzliwości.

Rozmawiał: Roman Szewczyk

I Regionalne Forum Gospodarcze – Inwestycje Przyszłości Jarocin 2025, odbyło się 21 listopada. Zgromadziło przedsiębiorców, samorządowców oraz przedstawicieli bankowego sektora spółdzielczego. Banki Spółdzielcze SGB były sponsorem wydarzenia. Forum obejmowało sesje plenarne i panele tematyczne z udziałem ekspertów SGB-Banku, BS Jarocin, SGB Leasing i SGB Faktoring. Dyskusje dotyczyły rozwoju regionu oraz inwestycji w zieloną gospodarkę i OZE.
Jednym z głównych mówców był Jacek Walkiewicz – gość Forum.

SALTUS | 30 lat
UBEZPIECZENIA



Z okazji Świąt Narodzenia Pańskiego składamy Państwu
serdeczne życzenia pokoju, nadziei i miłości.

Co roku ten szczególny czas przypomina nam o sile wiary,
dobra oraz bliskości i wzajemnej troski.

W SALTUS Ubezpieczenia dbamy o bezpieczeństwo,
a także o to, aby towarzyszyły nam tradycyjne wartości:
odpowiedzialność, uczciwość i szacunek.

Dziękujemy Państwu za kolejny rok owocnej współpracy, opartej na zaufaniu,
wzajemnym zrozumieniu oraz wspólnym dążeniu do stabilnego rozwoju
sektora bankowości spółdzielczej.

Niech nadchodzący rok przyniesie Państwu satysfakcję z podejmowanych
działań, wiele sukcesów zawodowych oraz pomyślność w realizacji
strategicznych celów, a także spokój i pewność w podejmowaniu
codziennych decyzji.

Zarząd i Pracownicy
SALTUS Ubezpieczenia

saltus.pl

Wesołych Świąt

Spółdzielcza tarcza zaufania

Bezpieczeństwo, które procentuje

Rozmowa z **Michałem Ołdakowskim**,
prezesem Zarządu Spółdzielczego Systemu Ochrony SGB

Spółdzielczy System Ochrony SGB powstał, żeby zapewnić stabilność i bezpieczeństwo bankom spółdzielczym. Jak wypełnia on swoją misję?

Od początku działania System Ochrony miał jeden zasadniczy cel: zapewnienie płynności i wypłacalności wszystkim swoim uczestnikom. Dziś, z perspektywy dekady, mogę powiedzieć, że mechanizmy, które wspólnie zaprojektowaliśmy – audyt, monitoring ryzyka, prewencja, wsparcie restrukturyzacyjne i fundusz pomocowy – po prostu działają. W efekcie żaden klient banku spółdzielczego objętego systemem ochrony nie stracił swoich oszczędności, nawet w sytuacjach skrajnie trudnych.

Jednocześnie udało się stworzyć kulturę współpracy, odpowiedzialności i wysokich standardów zarządzania ryzykiem. To wszystko przełożyło się na realną stabilność – zarówno w okresach kryzysowych, jak

pandemia COVID-19, jak i wtedy, gdy część banków potrzebowała wsparcia restrukturyzacyjnego.

Gdy ponad 10 lat temu powstawały systemy ochrony, niektórzy bankowcy obawiali się ograniczenia niezależności. Czy po dekadzie zgadza się pan z tym stwierdzeniem?

To była naturalna obawa – każda nowa instytucja nadzorcza lub wspierająca budzi pytania o zakres ingerencji. Ale historia pokazała coś zupełnie innego. IPS-SGB nie ograniczył niezależności banków. Przeciwnie, zabezpieczył ich samodzielność. Zawsze podkreślamy podmiotowość uczestników: my nie zarządzamy bankami, ale wspieramy je tam, gdzie wymaga tego bezpieczeństwo klientów. Dajemy narzędzia, wiedzę, audytujemy, przygotowujemy regulacje wzorcowe i pomagamy je wdrażać, ale decyzje biznesowe pozostają po stronie poszczególnych banków. Oczywiście w sytuacjach, w których identyfikujemy realne zagrożenie dla stabilności funkcjonowania banku, nasze działania są widoczne. Taka jest nasza rola, a podejmowanie odpowiednich działań mamy wpisane w umowę systemu.

Zawsze podkreślamy podmiotowość uczestników: my nie zarządzamy bankami, ale wspieramy je tam, gdzie wymaga tego bezpieczeństwo klientów.

Od samego początku zwracaliśmy też uwagę na to, by nasze działania związane z zapewnieniem bezpieczeństwa nie sparaliżowały działalności banków. Działamy tak, ponieważ uważamy, że brak rozwoju jest również istotnym ryzykiem biznesowym. Musi to jednak być rozwój bezpieczny, oparty o rzetelne rozpoznanie i zarządzenie ryzykiem. Jestem przekonany, że do tej pory udawało nam się godzić potrzebę ograniczania nadmiernego ryzyka z rozwojem. Świadczą o tym twarde dane finansowe: wzrost sum bilansowych, depozytów i kredytów. Kiedy zaczynaliśmy działalność w 2015 roku zagregowana suma bilansowa banków wynosiła 36,3 mld zł, dzisiaj to 94,8 mld zł a dynamika w tym okresie wyniosła 261% podczas gdy w bankach komercyjnych 231%.

Jeszcze wyraźniejsze różnice widać w rozwoju działalności kredytowej. Należności sektora niefinansowego i samorządowego w 2015 roku wynosiły ok. 22 mld zł, aktualnie to 38,4 mld zł, a dynamika wyniosła 175% w porównaniu z poziomem 131% w bankach komercyjnych. Warto podkreślić, że została zachowana lepsza niż na rynku jakość portfeli kredytowych – wskaźnik szkodowości wynosi obecnie 4,2% (w 2015 roku był zbliżony i wynosił 3,92%) w bankach komercyjnych 4,5%. Istotnie wzrósł natomiast poziom orezerwowania z ok. 33% do 69%.

Jest pan prezesem IPS-SGB od 2019 roku. Jakie było największe wyzwanie w tym okresie?

Najtrudniejsza była z pewnością restrukturyzacja Banku Spółdzielczego w Przemkowie. Bank przystąpił do systemu nie ujawniając swojej rzeczywistej sytuacji, a skala problemów była ogromna. Jednocześnie fundusz pomocowy był już wcześniej naruszony przez inną restrukturyzację.

W systemach ochrony niedopuszczalna jest upadłość uczestnika. W tamtym okresie byliśmy szczególnie wrażliwi – wybuchła właśnie pandemia i upadłość mogłaby podważyć zaufanie do całego systemu bankowego. Dzięki współpracy z BFG, SGB-Bankiem oraz KNF udało się przeprowadzić przymusową restrukturyzację, chroniąc klientów i stabilność sektora. Żaden z klientów banku nie stracił w jej wyniku swoich oszczędności.

Największą satysfakcję daje mi jednak fakt, że udało się zbudować zespół profesjonalistów, którzy rozumieją ideę spółdzielczości i chcą ją rozwijać. Bez nich żaden z sukcesów ostatnich lat nie byłby możliwy.

Czy zasady solidarności i samopomocy nabierają nowego znaczenia dziś – w dobie cyfryzacji i ostrej konkurencji rynkowej?

Zdecydowanie tak. Paradoks polega na tym, że im bardziej rozwinięty technologicznie jest rynek finansowy, tym większą wartość mają klasyczne spółdzielcze fundamenty: współpraca, rzetelność, zaufanie i odpowiedzialność za wspólne bezpieczeństwo.

Solidarność to nie slogan – ona realnie przekłada się na funkcjonowanie systemu ochrony. Zbudowaliśmy fundusz pomocowy, mechanizmy audytowe i prewencyjne, które chronią każdego uczestnika. Cała umowa Systemu Ochrony SGB, mająca charakter wielostronny, jest potwierdzeniem solidarności banków Spółdzielczej Grupy Bankowej. Ta wspólnota bezpieczeństwa jest siłą, której banki komercyjne nie mają.

Jak zmieniające się otoczenie regulacyjne, technologiczne i rynkowe wpłynie na funkcjonowanie IPS-SGB w kolejnych latach? Jakie obszary będą kluczowe?

Niewątpliwym wyzwaniem są nadmierne i często nieproporcjonalne regulacje. Banki spółdzielcze są małe i nieskomplikowane, a przepisy często tworzone są z myślą o dużych, międzynarodowych grupach kapitałowych. Dlatego w Polsce i na poziomie europejskim walczymy o większą proporcjonalność – i mamy tu już konkretne sukcesy, jak korzystne zmiany dotyczące wskaźnika dźwigni lub składki na BFG, czy też zwolnienie ze stosowania wskaźnika WFD. Mamy nadzieję, że kolejne uproszczenia przed nami.

Największą satysfakcję daje mi fakt, że udało się zbudować zespół profesjonalistów, którzy rozumieją ideę spółdzielczości i chcą ją rozwijać. Bez nich żaden z sukcesów ostatnich lat nie byłby możliwy.

Kolejnym, absolutnie kluczowym obszarem jest cyfryzacja. Od lat cyfryzujemy i automatyzujemy własne procesy w IPS-SGB. Zachęcamy do tego banki spółdzilecze i wspieramy również działania banku zrzeszającego w tym zakresie.

W kolejnych latach dużą uwagę będziemy przykładać do cyberbezpieczeństwa i rozwoju audytów ICT, automatyzacji procesów analitycznych i audytowych, dalszego rozwoju kompetencji w bankach – edukacji, szkoleń, webinarów i doradztwa. Bardzo

liczę też na rozwój produktów, usług i procesów bankowych. W tym zakresie oczywiście wiodącą rolę odgrywa SGB-Bank – my będziemy aktywnie wspierać te prace z perspektywy bezpieczeństwa i właściwego zarządzania ryzykiem.

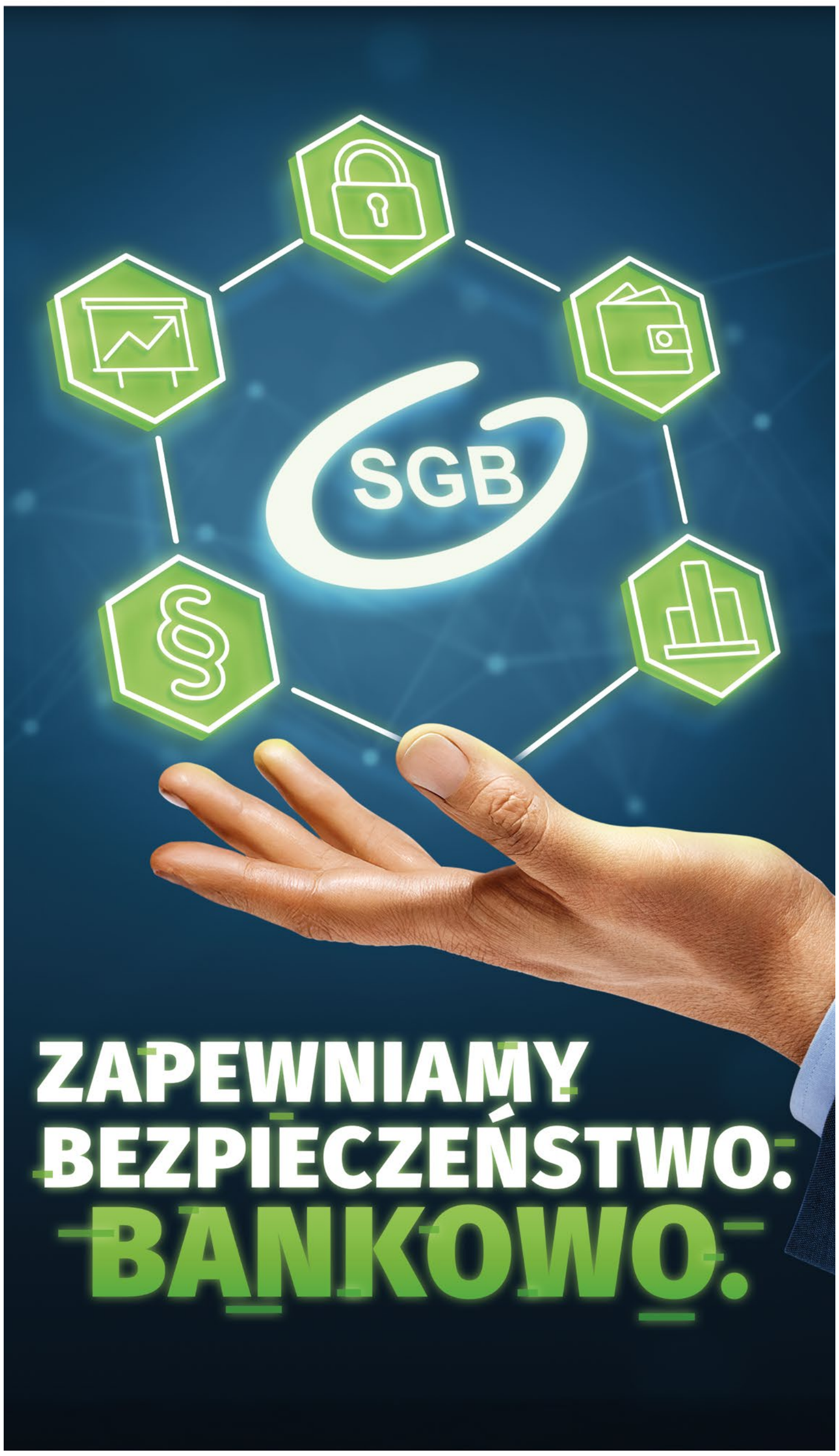
Nowe przepisy CIT i kolejne obniżki stóp procentowych oznaczają spadek rentowności sektora. Czy to dobry moment, by przyspieszyć konsolidację banków spółdzielczych?

Zmiana otoczenia prawnego i spadające stopy procentowe rzeczywiście będą wpływać na wyniki banków. Ale konsolidacja powinna być zawsze decyzją strategiczną, przemyślaną, a nie wymuszoną chwilową sytuacją. IPS-SGB ma doświadczenie w prowadzeniu procesów łączeniowych tam, gdzie były one konieczne – natomiast nie jesteśmy zwolennikami konsolidacji „dla samej konsolidacji".

Każdy bank jest inny, działa w innym otoczeniu lokalnym, ma własnych klientów i własne ambicje. Nasza misja polega na tym, by zapewnić im bezpieczne warunki rozwoju – a nie podsuwać jedną „uniwersalną" receptę. Jeżeli pojawią się sytuacje, w których konsolidacja będzie najlepszym rozwiązaniem – oczywiście będziemy wspierać te procesy. Ale nie uważam, żeby była to odpowiedź na wszystkie wyzwania rynkowe.

Myślę, że dzisiaj najważniejsze jest wykorzystanie bardzo dobrych fundamentów (wysokich współczynników kapitałowych, znakomitych wyników, dobrej jakości portfeli kredytowych) do budowy nowoczesnego, bezpiecznego biznesu. Niezwykle istotna w tym kontekście jest współpraca zrzeszeniowa, realizowanie wspólnych procesów w jak największym zakresie i dalsza aktywizacja sprzedaży.

iPS SGB SPÓŁDZIELCZY
System Ochrony SGB



FOT. ARCHIWUM IPS-SGB

Cała umowa Systemu Ochrony SGB, mająca charakter wielostronny, jest potwierdzeniem solidarności banków Spółdzielczej Grupy Bankowej. Ta wspólnota bezpieczeństwa jest siłą, której banki komercyjne nie mają.

Z okazji 10-lecia IPS-SGB i zbliżającego się końca 2025 roku – czego życzyłby pan bankom spółdzielczym i ich pracownikom?

Przede wszystkim odwagi i determinacji. Współczesny rynek finansowy bardzo szybko się zmienia. Jestem przekonany, że bankowość spółdzielcza ma ogromny potencjał, jeśli będzie rozwijać się w duchu spółdzielczym, ale z wykorzystaniem nowoczesnych narzędzi.

Życzę bankom, aby dalej budowały swoją siłę na wartościach: uczciwości, rzetelności, współpracy i przejrzystości – to one pozwalają zdobywać zaufanie klientów.

Pracownikom życzę satysfakcji z pracy i poczucia dumy z tego, że wspólnie tworzymy stabilny i bezpieczny system ochrony, który realnie chroni banki i oszczędności ich klientów.

A nam wszystkim – by kolejne lata były czasem mądrego, bezpiecznego rozwoju, innowacji i wspólnych sukcesów, bo siłą spółdzielczości jest właśnie współdziałanie.

Rozmawiał: Roman Szewczyk

Jubileusz ludzi, którzy budują bezpieczeństwo

Obchody jubileuszu dziesięciolecia IPS-SGB miały wyjątkowo uroczysty charakter. 19 listopada br., w gościnnych progach hotelu Novotel Centrum w Poznaniu, tam, gdzie 10 lat temu została podpisana Umowa Systemu Ochrony SGB, pojawiło się wielu znamienitych gości. Uświetnili swoją obecnością obchody jubileuszu: przedstawiciele Uczestników Systemu Ochrony SGB, instytucji sieci bezpieczeństwa finansowego, jednostki zarządzającej Systemem Ochrony Zrzeszenia BPS, izb gospodarczych, partnerzy biznesowi oraz wyróżnieni pracownicy IPS-SGB. Wśród gości nie zabrakło również tych, którzy jako pierwsi w Polsce tworzyli lub wspierali ten nowatorski wówczas projekt.

W trakcie jubileuszowych wystąpień podkreślano, że dekada istnienia Systemu Ochrony SGB to przede wszystkim czas stabilnej współpracy, zaufania i konsekwentnej aktywności osób odpowiedzialnych za bezpieczeństwo finansowe całego zrzeszenia SGB. Istotne jest, że podkreślali ten fakt przedstawiciele sieci bezpieczeństwa finansowego. Zwracano uwagę, że IPS stał się trwałym elementem architektury bezpieczeństwa sektora banków spółdzielczych, opartym na współodpowiedzialności, zaufaniu i solidarności instytucji.

Uczestnicy uroczystości wielokrotnie akcentowali, iż siłą zrzeszenia SGB jest zdolność do działania wspólnego, przy jednoczesnym zachowaniu lokalnej tożsamości i autonomii banków spółdzielczych. Bezpieczeństwo finansowe nie jest stanem danym raz na zawsze, lecz procesem wymagającym nieustannej aktywności i czujności, współpracy oraz dostosowywania się do zmieniających się warunków rynkowych.

Podkreślano, że w świecie rosnącego ryzyka — regulacyjnego, technologicznego i geopolitycznego — systemy ochrony instytucjonalnej odgrywają kluczową rolę w utrzymaniu zaufania do sektora bankowego.

Były wspomnienia, zabawa i wspólne zdjęcia, a to wszystko w radosnej atmosferze. Zresztą, zobaczcie sami.

Jubileusz czas zacząć …

Trochę historii …

Prowadzący jubileusz stanęli na wysokości zadania …

Były podziękowania, nagrody i wyróżnienia …

Kto drzewkiem wojuje …

Przyszedł czas na tort jubileuszowy …

Działamy razem z SGB-Bankiem i …

… Systemem Ochrony Zrzeszenia BPS.

Była okazja do spotkania z pracownikami IPS-SGB …

oraz do zrobienia zdjęć niekoniecznie na ściance …

Pod egidą systemu spółdzielczej ochrony

Ewa Kamińska
Wiceprezes Zarządu IPS-SGB

dr hab. Michał Jurek
Dyrektor Departamentu Monitorowania Ryzyka i Restrukturyzacji IPS-SGB

W listopadzie 2025 r. minęło dziesięć lat od chwili powstania Systemu Ochrony SGB, na czele z IPS-SGB. Dobra to okazja, aby w codziennej krzątaninie, związanej z realizacją bieżących wyzwań, zatrzymać się, spojrzeć wstecz i zastanowić, co udało się w tym czasie osiągnąć.

Utworzenie Systemu było krokiem w nieznane. Nie było w Polsce dotąd instytucji, która działałaby w taki sposób – jako podmiot utworzony przez banki spółdzielcze po to, by je wspierać w bieżącej działalności, zapewnić właściwy monitoring wszystkich rodzajów ryzyka oraz zapobiegać powstawaniu sytuacjom trudnym, które mogłyby narazić na szwank całe Zrzeszenie SGB. Nie było też pracowników, infrastruktury, siedziby. Była – tylko i aż – kartka papieru, długopis i grupa ludzi z pomysłami oraz z zapałem, niezbędnym do tego, by idee przekuć w rzeczywistość. I tak powstał System Ochrony SGB, pierwszy polski instytucjonalny systemem ochrony, utworzony 23 listopada 2015 r., a także jednostka, która nim zarządza, czyli właśnie IPS-SGB.

> Siłą Systemu Ochrony SGB jest prewencja — umiejętność dostrzegania ryzyka, zanim ktokolwiek zdąży poczuć jego ciężar.

IPS-SGB trzyma rękę na pulsie

Dziesięć lat to nie tak znowu dużo czasu. A mimo to udało się w tym okresie stworzyć sprawnie działającą instytucję, która w sposób cykliczny realizuje wymagane przez nadzorcę i banki spółdzielcze analizy ryzyka i badania audytowe. Przygotowuje i nieustanie realizuje regulacje wzorcowe, niezbędne w działalności banków spółdzielczych. Udziela uczestnikom Systemu pomocy wtedy, gdy to niezbędne, i to nie tylko finansowej, ale i prawnej oraz merytorycznej. Organizuje szkolenia i kursy. Do tego trzyma rękę na pulsie, jeśli chodzi o krajowe i zagraniczne zmiany legislacyjne. Powstrzymuje te, które mogłyby mieć negatywny wpływ na sytuację swoich członków, a wspiera wdrożenie tych z nich, które ułatwiają bieżące funkcjonowanie banków spółdzielczych, zgodnie z postulatem proporcjonalności.

W dotychczasowej historii IPS-SGB było kilka punktów zwrotnych. Należało do nich z pewnością skuteczne zapobieżenie upadłości dwóch uczestników poprzez zastosowanie niestandardowych mechanizmów pomocowych. Dość wspomnieć, że w jednym z tych przypadków pierwszy raz w Polsce zastosowana została procedura przymusowej restrukturyzacji z zaangażowaniem finansowym Bankowego Funduszu Gwarancyjnego. Nikt wcześniej tego nie zrobił. Tymczasem proces został niemal w całości przygotowany od strony merytorycznej przez pracowników IPS-SGB i SGB-Banku.

IPS-SGB wspierał też swoich członków w niełatwym czasie pandemii COVID-19. Pracownicy Spółdzielni opracowali autorskie narzędzia, służące zarządzaniu restrukturyzacją banku w obszarze biznesowym. Przygotowywali organy korporacyjne banków spółdzielczych do przeprowadzenia procesów łączeniowych tam, gdzie nie było już szans na samodzielną sanację. Tam zaś, gdzie podejmowane były samodzielne próby naprawy, pomagali w sporządzeniu wewnętrznych planów naprawy. W kulminacyjnym punkcie realizowane były 24 takie plany. Większość banków spółdzielczych zakończyła już ich realizację, wdrażając odpowiednie opcje naprawcze i w sposób trwały ograniczając ryzyko.

> Dziesięć lat po starcie IPS-SGB wciąż udowadnia, że wizja kilku ludzi z kartką papieru może stać się tarczą chroniącą całe Zrzeszenie.

Minione dziesięć lat to również

ciągły rozwój badań audytowych. W okresie pandemii wypracowano hybrydową formułę przeprowadzania tych badań i udoskonalono mechanizm cyklicznego raportowania informacji na temat efektywności realizacji zaleceń poaudytowych. Wypracowane rozwiązania, które udowodniły swoją skuteczność, stosowane są także i dziś. Dzięki temu możliwe jest znaczne skrócenie cyklu audytowego, co daje możliwość przeprowadzenia rocznie ponad 120 badań. Zespół audytu dał podstawy pod utworzenie wewnętrznego systemu informatycznego, który aktualnie usprawnia prace nie tylko audytorom, a ponadto umożliwia wyeliminowanie papierowego obiegu dokumentów.

Spółdzielczy System Ochrony SGB wpisał się już na stałe w obraz polskiego sektora bankowego. Jest instytucją obecną w codziennej działalności banków spółdzielczych. Nie byłoby tego sukcesu bez zbudowania solidnego fundamentu, którym jest zgrany, rozumiejący się i działający we wspólnym celu zespół pracowników. Niemal połowa obecnego składu osobowego jest w IPS-SGB od samego początku, stanowiąc żywą skarbnicę pamięci i doświadczeń zebranych w trakcie pionierskich pierwszych lat działania instytucji.

Skuteczna prewencja z wykorzystaniem mechanizmów

Celem Spółdzielczego Systemu Ochrony SGB jest skuteczna prewencja z wykorzystaniem mechanizmów zapobiegania nadmiernemu ryzyku, aby żaden uczestnik nie był zagrożony upadłością. Jak mawia znane powiedzenie, łatwiej zapobiegać, niż gasić. I takie właśnie motto przyświeca wszystkim działaniom, podejmowanym przez IPS-SGB. Dzięki temu, nawiązując do tytułu felietonu, IPS-SGB jest tarczą, która chroni Zrzeszenie SGB i daje odpór zagrożeniom.

Spółdzielczy System Ochrony SGB nie spoczywa jednak na laurach i wciąż się doskonali. Dzięki pokonaniu wyzwań, piętrzących się od samego początku funkcjonowania instytucji, udało się wypracować unikalny mechanizm identyfikacji i rozpoznawania ryzyka, i to na długo zanim dojdzie do jego faktycznej materializacji. To zaś umożliwia naprawę sytuacji z odpowiednim wyprzedzeniem i odpowiednie przygotowanie się do nadchodzących zmian. Jak bowiem mawiał Sun Zi w „Sztuce walki": Osiągnąć sto zwycięstw w stu bitwach nie jest szczytem umiejętności. Szczytem umiejętności jest pokonanie przeciwnika bez walki. Marzeniem IPS-SGB jest w końcu rzeczywiste wdrożenie zasady proporcjonalności w zasadach funkcjonowania banków spółdzielczych, a to jak pokazały kilkuletnie doświadczenia, jest możliwe głównie poprzez zmianę przepisów prawa – pierwsze światełka w tunelu już się pokazały.

Takiego właśnie dalszego skutecznego zapobiegania powstawaniu trudnych sytuacji oraz spełniania marzeń wszystkim Czytelnikom i sobie życzymy. ●

Tak rodził się system bezpieczeństwa

Dziesięć lat temu powstał pierwszy w Polsce System Ochrony Instytucjonalnej. To był moment przełomowy – nie tylko dla sektora bankowości spółdzielczej, ale również dla całego rynku finansowego. Dziś, z perspektywy dekady, warto wrócić do tamtych chwil, emocji i decyzji, które kształtowały nową architekturę bezpieczeństwa.
Ewa Kamińska, wiceprezes Zarządu IPS-SGB, postanowiła porozmawiać z osobami, które od pierwszego dnia były współtwórcami tego projektu. Pytała o najtrudniejsze wybory, o problemy, z którymi musieli się mierzyć, oraz o to, jak pamiętają dynamikę wydarzeń sprzed lat. To opowieść o odpowiedzialności, współpracy i wizji, która dzięki odwadze wielu osób stała się rzeczywistością.

Liderka w cieniu trudnych decyzji

ELŻBIETA NOWAKOWSKA-AKKERMANS, przewodnicząca Rady Zrzeszenia w latach 2013-2016

W okresie organizacji systemu ochrony była pani przewodniczącą Rady Zrzeszenia. Co pani zdaniem sprawiało największą trudność przy organizacji systemu?

Moją najważniejszą rolą było przewodniczenie Zgromadzeniom Prezesów w taki sposób, aby z przekonaniem, czyli skutecznie, podjęte zostały wszystkie decyzje zatwierdzające zmiany w istniejących regulacjach oraz wprowadzenie nowych, niezbędnych i związanych z organizacją systemu.
Innymi zadaniami było uczestnictwo w pracach międzyzrzeszeniowych z radami SGB i Zrzeszenia BPS w zakresie uzgodnienia celów systemu, pozyskania informacji o istniejących rozwiązaniach w Europie, ustalenia koniecznych zmian w Ustawie o funkcjonowaniu banków spółdzielczych. Między nami, wspólnie z ZBP, KZBS, BPS, Związkami Rewizyjnymi, a zespołem z UKNF, dyskutowane były graniczne wymogi, które muszą być spełnione przez system ochrony. Rada Zrzeszenia poddawała analizie i zatwierdzeniu wszystkie wypracowywane przez zespoły i grupy

Z perspektywy czasu jestem dumna, że sektor wybrał tę drogę spółdzielczej współpracy, gwarantującą sobie wzajemnie bezpieczeństwo.

robocze konkluzje oraz dokumenty przed ich przedstawieniem na Zgromadzeniu Prezesów.
A nie były to wcale proste zadania, gdyż cały proces lub jego elementy napotykały na opór wielu banków spółdzielczych. Bardzo często w dyskusjach z prezesami zarzucano mi stronniczość i reprezentowanie bardziej stanowiska SGB-Banku lub UKNF oraz brak wystarczającej postawy spółdzielczej. Uważano, że czasami zbyt stanowczo przewodniczę Zgromadzeniom Prezesów. Nie było entuzjazmu grupy, jaki odczuwałam przy zakładaniu GBW czy KZBS.
Głównymi wnioskami, które wynikały z tych dyskusji były obawy przed ograniczeniem własnych lokalnych strategii produktowych i cenowych. Banki wręcz uważały, że powstanie systemów ochrony to zmierzanie w kierunku konsolidacji Grupy SGB.
Całą posiadaną wówczas wiedzę z procesu organizacji IPS wykorzystywałam do uzasadniania korzyści na zasadzie analizy SWOT, a ponieważ sama wewnętrznie byłam przekonana do tego rozwiązania, to łatwiej mi było argumentować.
Po zatwierdzeniu przez Zgromadzenie Prezesów SGB dokumentacji systemu, kolejnym wyzwaniem okazało się osobiste stawiennictwo z prezesami Ryszardem Lorkiem i Adamem Skowrońskim przed pełnym składem Komisji Nadzoru Finansowego, celem uzasadnienia, a wręcz wybronienia zasadności i pozytywnego wpływu funkcjonowania systemu w zaproponowanej formie na bezpieczeństwo sektora bankowego.
Z perspektywy czasu jestem dumna, że sektor wybrał tę drogę spółdzielczej współpracy, gwarantującą sobie wzajemnie bezpieczeństwo.

Doświadczenie, które zaprocentowało

ZYGMUNT MIĘTKI, wiceprezes Zarządu SGB-Banku w latach 2006-2013

Był pan pierwszym szefem zespołu zajmującego się tworzeniem podstaw i reguł funkcjonowania systemu ochrony. Co panu najbardziej utkwiło w pamięci?

Gdy w wyniku uchwalenia regulacji unijnych (Dyrektywy CRD i Rozporządzenia CRR) powstała potrzeba utworzenia instytucjonalnego systemu ochrony w Spółdzielczej Grupie Bankowej, w zrzeszeniu istniała już wiedza i pewne doświadczenie w zakresie funkcjonowania systemów wzajemnego wsparcia.

Działanie funduszy samopomocowych w zrzeszeniach banków spółdzielczych było znane już od 1993 roku. W tamtym czasie Narodowy Bank Polski zobowiązał banki spółdzielcze zrzeszone w trzech niezależnych od BGŻ grupach, na czele z GBW, GBPZ i BUG do utworzenia funduszy samopomocowych w ramach każdego zrzeszenia. Decyzja NBP była następstwem pogarszającej się sytuacji ekonomicznej i płynnościowej w bankach spółdzielczych. Banki spółdzielcze zrzeszone z GBW utworzyły kilka funduszy samopomocowych, które na początku 1995 roku połączone zostały w jeden fundusz o nazwie Fundusz Powierzony, który na koniec tego roku został rozwiązany.

Dlatego w nowym otoczeniu prawnym ważnym zagadnieniem było to, aby tworząc nowy sytemu ochrony wykorzystać wiedzę i doświadczenie sprzed dwudziestu lat, w taki sposób aby nie popełnić błędów jakie popełniono na początku lat 90. Kluczowym tematem była forma prawna systemu ochrony, zwłaszcza w świetle zapisów ustawowych, które dopuszczały funkcjonowanie tzw. zrzeszenia zintegrowanego. Słabym elementem rozwiązania ze zrzeszeniem zintegrowanym było to, że stroną umów o udzielenie pomocy byłby bank zrzeszający (podobnie było na początku lat 90). Tym samym rezerwy celowe powstałe w wyniku braku zwrotu udzielonej bankowi spółdzielczemu pomocy, obciążały wynik finansowy banku zrzeszającego.

Opcją najbardziej czytelną z punktu widzenia organizacyjnego było utworzenie jednostki zarządzającej systemem ochrony jako odrębnego podmiotu gospodarczego, który spełniałby wszystkie oczekiwania w zakresie organizacyjnym i prawnym dla realizacji zapisów ustawowych.

Z kolei u sporej grupy banków spółdzielczych zrzeszenia SGB pojawiły się obawy, że samodzielna jednostka to będą dodatkowe koszty dla banków spółdzielczych, gdyż ze składek banków spółdzielczych trzeba będzie pokryć koszty jej funkcjonowania. Podnoszono także problem, który często jest obserwowany w takich sytuacjach, że nowy podmiot zaczyna żyć swoim życiem i nie zawsze spełnia pokładane w nim oczekiwania nakreślone w momencie jego tworzenia.

Chciałbym jeszcze wskazać na jeden problem, z którym się spotkałem na etapie tworzenia reguł i zasad funkcjonowania systemu ochrony. Na pewnym etapie prac w proces tworzenia systemu została włączona zewnętrzna kancelaria prawna, co okazało się niezbyt dobrą decyzją i co ostatecznie wydłużyło nasze działania. Zewnętrzna kancelaria prawna nie dysponowała potrzebną wiedzą na temat spółdzielczości bankowej i prawa unijnego w tym obszarze, a bez jej pozyskania nie dało się zrealizować projektu w wyznaczonym terminie. Czas przeznaczony na uzupełnienie wiedzy jej pracowników okazał się zbyt długi i mało efektywny. Ostatecznie, kolejna decyzja o zaangażowaniu kancelarii prawnej obsługującej zrzeszenie SGB, znacznie przyśpieszyła wypracowanie ostatecznej formuły funkcjonowania zrzeszenia z instytucjonalnym systemem ochrony.

W konsekwencji przyjęte rozwiązanie funkcjonowania zrzeszenia z instytucjonalnym systemem ochrony, a jednostki zarządzającej tym systemem w formie samodzielnego podmiotu – to jest spółdzielni osób prawnych okazało się rozwiązaniem trafionym.

> Doświadczenie sprzed dwudziestu lat pomogło nam stworzyć instytucjonalny system ochrony, który okazał się rozwiązaniem trafionym dla całej Spółdzielczej Grupy Bankowej.

Gdzie rodził się konsensus

MAREK BANASZAK, prezes Zarządu Powiatowego Banku Spółdzielczego w Gostyniu

Był pan jednym z członków zespołu roboczego składającego się z przedstawicieli banków zrzeszonych w SGB. Wspierał pan prace zespołu powołanego w SGB-Banku, uczestniczył w spotkaniach z Urzędem Komisji Nadzoru Finansowego. Jaka część zasad funkcjonowania systemu była najtrudniejsza do uzgodnienia?

Trudności w rozmowach wśród uczestników zespołu jak i z UKNF najczęściej koncentrowały się wokół aspektów, które wymagały odejścia od standardowych zasad indywidualnego nadzoru

Wyzwaniem było określenie parametrów wzajemnego gwarantowania płynności i wypłacalności w taki sposób, aby to gwarantowanie było w praktyce wykonalne.

i przejścia na nadzór skonsolidowany w ramach systemu ochrony. Wyzwaniem było również określenie parametrów wzajemnego gwarantowania płynności i wypłacalności w taki sposób, aby to gwarantowanie było w praktyce wykonalne.
Dyskusje toczyły się wokół pewności i automatyzmu wsparcia. Należało przekonać UKNF, że w przypadku problemów u jednego uczestnika, system ochrony jest w stanie szybko, skutecznie i automatycznie uruchomić wsparcie finansowe (płynnościowe lub kapitałowe) bez zbędnej zwłoki czy negocjacji. W ramach negocjacji musiały być precyzyjnie określone:

- wielkość funduszu pomocowego, którego system w momencie tworzenia jeszcze nie miał. Należało ustalić adekwatną wielkość funduszu pomocowego (który będzie gromadzony przez uczestników) i przekonać UKNF, że jest ona wystarczająca, aby pokryć potencjalne ryzyka w grupie,
- warunki udzielania pomocy. Należało ustalić w jakich sytuacjach, na jakich zasadach i pod jakimi warunkami (np. plan naprawy) będzie udzielane wsparcie. UKNF musiał mieć pewność, że pomoc będzie efektywna i nie pogorszy sytuacji pozostałych uczestników,
- warunki przystąpienia poszczególnych uczestników do sytemu. Koniecznym było określenie jednolitych kryteriów przystąpienia banku do systemu tj. należało wybrać i zdefiniować rodzaje oraz poziom wskaźników finansowych, których spełnienie jest konieczne, aby stać się uczestnikiem systemu. Nie było to proste zadanie, gdyż było wielu przyszłych uczestników o różnej specyfice działania, osiąganych wskaźnikach i sposobie liczenia tych wskaźników.

Udało się tak określić zasady działania systemu, że uzyskaliśmy zgodę UKNF na utworzenie Systemu Ochrony SGB, niemniej jednak UKNF w swej decyzji przedstawił jeszcze 14 dodatkowych warunków do spełnienia w określonym czasie przez System jak i przez jego uczestników.

Czas dojrzałej decyzji

BARBARA BOROWSKA, prezes Zarządu Banku Spółdzielczego w Gnieźnie

Bank, którym pani zarządza nie był jednym z Założycieli Systemu Ochrony SGB. Co zadecydowało o tym, że bank przystąpił do systemu w późniejszym, aczkolwiek trzeba przyznać, niezbyt odległym terminie?

Nie ukrywam, że jest to dla mnie dość kłopotliwe pytanie, i bynajmniej nie z powodu braku uzasadnienia odroczonej decyzji. Jest to jednak kwestia delikatnej natury, a przede wszystkim innej decyzyjności. Datę podpisania przez większość banków spółdzielczych i SGB-Bank umowy uczestnictwa w Systemie Ochrony SGB oraz moment formalnego przystąpienia naszego banku, w zasadzie oddzielały niepełne cztery miesiące, co jest stosunkowo krótkim okresem. Był to jednak czas niezbędny i przełomowy, aby usunąć istniejące jeszcze bariery wewnętrzne, przełamać utarte schematy i otworzyć się na nową rzeczywistość.
Trzeba podkreślić, że nie był to problem zanegowania koncepcji wspólnej troski nad płynnością finansową i wypłacalnością całej grupy, ani też nieracjonalny opór przed nową sytuacją zrzeszeniową. Dowodzi tego choćby fakt, że już w grudniu 2015 roku Zebranie Przedstawicieli banku wyraziło zgodę na jego uczestnictwo w Systemie Ochrony SGB. Chodziło raczej o to, aby wobec czegoś całkowicie nowego nie działać bez przekonania, z balastem zbyt wielu znaków zapytania i wątpliwości.
Z perspektywy czasu uważamy, że przystąpienie do Systemu Ochrony SGB po kilku miesiącach od chwili jego powołania, okazało się ostatecznie czymś pożytecznym dla banku. Była to bowiem w pełni świadoma i dojrzała decyzja, przedyskutowana w każdym możliwym jej aspekcie. Co więcej, można zaryzykować tezę, że dzięki lepszemu zrozumieniu i akceptacji nowej formuły współodpowiedzialności banków spółdzielczych, udało nam się szczelnie zamknąć pierwszy rozdział niepewności i emocji, aby dość szybko otworzyć nowy rozdział – bardziej zaangażowany, aktywny i konstruktywny.

Przystąpienie do Systemu Ochrony SGB po kilku miesiącach od chwili jego powołania, okazało się ostatecznie czymś pożytecznym dla banku. Była to bowiem w pełni świadoma i dojrzała decyzja, przedyskutowana w każdym możliwym jej aspekcie. Co więcej, można zaryzykować tezę, że dzięki lepszemu zrozumieniu i akceptacji nowej formuły współodpowiedzialności banków spółdzielczych, udało nam się szczelnie zamknąć pierwszy rozdział niepewności i emocji, aby dość szybko otworzyć nowy rozdział – bardziej zaangażowany, aktywny i konstruktywny.

Burze mózgów

MONIKA KLÓSKA, główna specjalistka, Departament Obsługi Prawnej i Administracji w IPS-SGB

Była pani jednym z pierwszych pracowników zatrudnionych w IPS-SGB, w dodatku w zespole odpowiedzialnym za administrację, kadry i obsługę prawną. Pamięta pani początki organizacji funkcjonowania spółdzielni? Jak wyglądały? Co najbardziej zapadło pani w pamięć?

Pamiętam tamte czasy, jakby to było… wczoraj. Wracam do nich z sentymentem. Początki funkcjonowania IPS-SGB to okres intensywnej pracy, ogromnego zaangażowania i prawdziwego ducha spółdzielczego.

Najbardziej pamiętne było uczucie, że tworzymy coś od podstaw. Były szybkie decyzje, elastyczność i poczucie wspólnego celu działania. Ze względu na małą liczbę pracowników, wszyscy znaliśmy się osobiście i mieliśmy bezpośredni wpływ na wiele spraw. Moja praca w Biurze Zarządu była szczególnie wymagająca, myśli były jednocześnie zajęte przez wiele tematów i spraw. Jednak mimo ogromnego natłoku obowiązków i presji, panowała sympatyczna atmosfera. Częste spotkania, wspólne „burze mózgów” i przekonanie, że budujemy coś trwałego, sprawiały, że praca przynosiła satysfakcję. Niejednokrotnie wspominamy przeróżne sytuacje, np. skąd wziąć na szybko ekspres do kawy, itd.

Najbardziej pamiętne było uczucie, że tworzymy coś od podstaw. Były szybkie decyzje, elastyczność i poczucie wspólnego celu działania. Ze względu na małą liczbę pracowników, wszyscy znaliśmy się osobiście i mieliśmy bezpośredni wpływ na wiele spraw.

Pierwsze lata ukształtowały fundamenty, na których IPS-SGB działa do dziś. Zawsze będę z rozrzewnieniem wspominać ten dynamiczny, pełen wyzwań, ale i satysfakcji czas.

Z korporacji do spółdzielni

AGNIESZKA JANC, wiceprezes Zarządu IPS-SGB

Dołączyła pani do zespołu IPS-SGB w pierwszej połowie 2016 roku, pełniąc rolę dyrektora Departamentu Audytu. Teraz jest pani wiceprezesem Zarządu nadzorującym audyt. Środowisko bankowości spółdzielczej było pani całkowicie obce, gdyż wcześniej zajmowała pani menadżerskie stanowiska w audycie dużego banku komercyjnego.
Co panią zaskoczyło w nowej pracy? Jakie różnice dostrzegła pani we współpracy z bankami spółdzielczymi w porównaniu z doświadczeniami wyniesionymi z banku komercyjnego? Ponieważ pewna praktyka funkcjonowania audytu była już ukształtowana w ramach jego działania w banku zrzeszającym, to czy było coś, co uznała pani za wymagające zmiany w pierwszej kolejności?

Właściwie wszystko było dla mnie w pewnym sensie zaskoczeniem. Najważniejsze – od razu zrozumiałam, jak wielka to będzie odpowiedzialność w porównaniu do zadań realizowanych do tej pory w banku komercyjnym. Może to trochę niektórych zdumiewać, ale jednak bank komercyjny – inaczej zorganizowany – nie polega aż tak fundamentalnie na funkcji audytu. Tymczasem w systemie ochrony to rola kluczowa – i to nie tylko dla indywidualnego banku spółdzielczego – ale przede wszystkim dla całego systemu, gdzie konsekwencje nadmiernego ryzyka jednej instytucji mogą odczuć wszyscy.

Cieszę się, że kontakt z ludźmi jest tu bliższy, rozmowy bezpośrednie i mają bardziej „ludzką twarz”, że nie ma tutaj tak wielu pośredników w dotarciu do kierownictwa banku, a informacja zwrotna jest bardziej szczera, chociaż czasami niezwykle bezpośrednia – co ją mocno odróżnia od korporacji.

Współpraca z bankami spółdzielczymi także okazała się inna – chociaż akurat tego się spodziewałam. Jest to relacja znacznie bliższa i „mniej korporacyjna” niż kultura pracy znana przeze mnie do tej pory. Nie twierdzę, że kultura pracy w dużej instytucji jest gorsza – jest po prostu zupełnie inna. I muszę jednoznacznie stwierdzić, że pod tym względem lepiej się czuję w środowisku spółdzielczym.

Cieszę się, że kontakt z ludźmi jest tu bliższy, rozmowy bezpośrednie i mają bardziej „ludzką twarz”, że nie ma tutaj tak wielu pośredników w dotarciu do kierownictwa banku, a informacja zwrotna jest bardziej szczera, chociaż czasami niezwykle bezpośrednia – co ją mocno odróżnia od korporacji. Podobnie jest w Spółdzielni, w grupie moich koleżanek i kolegów z Departamentu Audytu. Myślę, że bliskość pracy z ludźmi, duże i wspólne poczucie odpowiedzialności za to co robimy, ale też ogromne zaangażowanie, poczucie współodpowiedzialności i tego, że od naszej pracy wiele zależy – to prawdziwe wartości, które charakteryzują nasz zespół. A do tego koniecznie trzeba dodać prawdziwą współpracę w zespole, wysoki poziom empatii i – tak mi się przynajmniej wydaje – brak niezdrowej rywalizacji, co nie zawsze jest oczywiste w korporacji.

To co mnie zaskoczyło mocno i co zmieniałam w pierwszej kolejności – to metodyka audytu – trochę za mało nastawiona na ryzyko, a także wszelkie przestarzałe metody pracy – jak np. papierowe raporty, ręczne podpisy, parafki itd. W związku z tym, największym wyzwaniem na początku było stworzenie koncepcji, praca z firmą informatyczną, a następnie wdrożenie systemu do obsługi procesów audytowych oraz wydawania zaleceń. To się udało i istotnie usprawniło naszą pracę. Wszystko to nie byłoby możliwe bez moich menedżerów i pracowników. Zrozumieliśmy się w zasadzie od początku i dlatego tak wiele udało się wspólnie wypracować lub zmienić.

Od niepewności do pewności

JACEK BALDY, prezes Zarządu Banku Spółdzielczego w Wołczynie

Był pan jednym z członków zespołu roboczego, składającego się z przedstawicieli banków zrzeszonych w SGB. Wspierał pan prace zespołu powołanego w SGB-Banku oraz wsłuchiwał się w głosy swoich koleżanek i kolegów z innych banków. Zmieniona ustawa o funkcjonowaniu banków spółdzielczych wskazywała różne możliwe formy działania zrzeszeń. Co pana koleżanki i koledzy sądzili o planowanych zmianach?

Generalnie dla wszystkich była to wielka niewiadoma. Wśród osób pamiętających jeszcze czasy BGŻ przeważała obawa przed częściową utratą ciężko wywalczonej niezależności. Z kolei młodsi pracownicy zastanawiali się, czy zmiany nie doprowadzą do nadmiernej kontroli poprzez limity, wzorce i inne rozwiązania, które mogą ograniczać rozwój. Ogólnie rzecz biorąc, entuzjazmu wobec powstania IPS w środowisku nie było – choć mieliśmy świadomość, że procesu tego nie da się uniknąć.

Naturalne jest, że w pierwszej kolejności dostrzegamy trudności, a rzadziej korzyści wynikające z nowych rozwiązań. Obawy zarządów podzielały również rady nadzorcze. Dlatego, gdy zarządy przekonały się do przystąpienia do IPS, musiały zdobyć także poparcie organów nadzorczych i zebrań przedstawicieli.

Nie ułatwiała tego silna presja – zwłaszcza w zrzeszeniu BPS, które, nie wiedzieć czemu, przedstawiało się jako bardziej „wolnościowe” – na wybór tzw. trzeciej drogi, czyli utworzenia banku apeksowego. Dziś wiemy, jak się ta koncepcja zakończyła, choć wówczas wielu z nas – nawet bez deklaracji ewentualnego przystąpienia – kibicowało temu rozwiązaniu z czystej ciekawości: jak ta grupa poradzi sobie w praktyce i czy w przyszłości mogłaby stać się realną alternatywą.

W naszym banku po wielu dyskusjach osiągnęliśmy jednomyślność, choć – jak mawialiśmy – „głosowaliśmy, ale nie cieszyliśmy się”. Wiem jednak, że w wielu bankach głosy były podzielone aż do samego końca, choć finalnie większość zdecydowała się na wejście do IPS.

Dziś, po 10 latach, można powiedzieć, że żadne z tamtych obaw się nie ziściły. Alternatywy praktycznie nie ma, a początkowe lęki dawno zniknęły. Mimo trudnego startu – mam tu na myśli „trupy w szafie” w kilku bankach, które sporo nas kosztowały – powstanie IPS należy ocenić pozytywnie.

W środowisku nie było entuzjazmu wobec powstania IPS, choć wszyscy mieli świadomość, że tego procesu nie da się uniknąć. Dziś widać wyraźnie, że obawy sprzed dekady nie znalazły potwierdzenia.

Od pustego pliku do systemu ochrony

EWA KAMIŃSKA, wiceprezes Zarządu IPS-SGB

Pamiętam jak w komputerze otworzyłam pusty plik w programie Word, napisałam tytuł, i… co dalej. Najtrudniej zacząć i opracować ogólną koncepcję, potem pozostaje już wypełnienie tej koncepcji treścią. Nie ukrywam, że wykorzystałam moje doświadczenia z tworzenia zasad zarządzania ryzykiem dla banków spółdzielczych czyli określić: które ryzyka będą istotne, jak gromadzić dane do pomiaru, jak mierzyć ryzyko, jakie będą obowiązywać limity i informacja zarządcza. Przygotowywanie czegoś od zera z pewnością jest bardzo trudne, potem już łatwiej aktualizować i zmieniać.

Kolejny etap, który mam w pamięci, to początki działalności spółdzielni. Podczas naszego jubileuszu, prezes Michał Ołdakowski wspominał o trudnych początkach formalnego zatwierdzenia spółdzielni przez Krajowy Rejestr Sądowy. Do początku lutego 2016 roku Zarząd (w którym powierzono mi funkcję wiceprezesa) funkcjonował jako Komisja Organizacyjna. Nie mając jeszcze pracowników, musieliśmy już realizować zadania przypisane jednostce zarządzającej Systemem Ochrony SGB, w tym wykonać zadania określone w decyzji KNF, o której wspomniał już prezes Marek Banaszak. Pierwszą analizę ryzyka Systemu, według stanu na koniec grudnia 2025 roku sporządzałam razem z Michałem Ołdakowskim. Pamiętam, że w przededniu wysyłki raportu do UKNF wyszliśmy z pracy przed północą, a następnego dnia ówczesny prezes Adam Skowroński zażartował, że skoro tak dobrze nam idzie, to możemy zoptymalizować planowany poziom zatrudnienia.

Pamiętam jak w komputerze otworzyłam pusty plik w programie Word, napisałam tytuł, i… co dalej. Najtrudniej zacząć i opracować ogólną koncepcję, potem pozostaje już wypełnienie tej koncepcji treścią.

Na koniec – trochę moich wspomnień. Od początku byłam członkiem powołanego w SGB-Banku zespołu projektowego i brałam udział w tworzeniu zasad funkcjonowania systemu ochrony. Szczególnie jestem przywiązana do załącznika do umowy, określającego zasady monitorowania ryzyka poszczególnych uczestników systemu. Należało szczegółowo rozpisać wymóg rozporządzenia CRR, mówiący że: „instytucjonalny system ochrony ma odpowiednie i jednakowo zorganizowane mechanizmy monitorowania i klasyfikowania ryzyka…”.

Na koniec, mam nadzieję, że jak już będę wieloletnim emerytem, to na jednym z jubileuszy, ktoś poprosi „staruszkę Kamińską”, aby opowiedziała coś o początkach systemu i spółdzielni.

POKAŻ SIĘ TAM, GDZIE BANKI SPÓŁDZIELCZE SZUKAJĄ ROZWIĄZAŃ

Ponad **10 000 profesjonalistów**

174 banki

Jeden e-magazyn

BANK SPÓŁDZIELCZY

Twoje miejsce
Twój target
Twoja reklama

SPRAWDŹ TO!

Reklama: **Monika Zarębska** +48 **608 339 937**

BS
AKADEMIE SGB

WIĘCEJ NIŻ ROZWÓJ – BUDUJEMY GALAKTYKĘ MOŻLIWOŚCI

Grażyna Koziołek
SGB-Bank

Rozwój umiejętności i kompetencji eksperckich nie jest w bankowości spółdzielczej dodatkiem do strategii – jest koniecznością i wyzwaniem.
W świecie, który z każdym rokiem przyspiesza, nie wystarczy już być ekspertem finansowym. Inspiracji warto szukać szerzej: w technologii, psychologii, naukach behawioralnych, komunikacji, a nawet w… kosmologii. Bo dzisiejsze kompetencje przypominają galaktykę: są złożone, dynamiczne, stale się rozszerzają i wzajemnie przenikają.

Galaktyka kompetencji przyszłości

Przyszłość pracy w bankowości wymaga dużo więcej niż pojedynczych szkoleń. Potrzebuje harmonii trzech elementów:

- WIEDZY, która pozwala zrozumieć procesy, merytorykę i regulacje,
- UMIEJĘTNOŚCI, które umożliwiają działanie,
- POSTAW, które kształtują odpowiedzialność, otwartość i gotowość na zmianę.

Patrząc z tej perspektywy, kompetencje przyszłości lokują się we wspólnym zbiorze wielu czynników:

- Cyberhigiena i bezpieczeństwo danych
- Myślenie analityczne
- Odporność psychiczna, relacje między zespołami oraz współpraca
- Zwinne przywództwo
- Rozumienie ESG i umiejętność przekładania go na praktykę biznesową
- Etyka cyfrowa i odpowiedzialność w świecie AI
- Budowanie relacji biznesowych

Te kompetencje stanowią mapę współczesnej „galaktyki możliwości” i wyznaczają kierunek rozwoju pracowników sektora finansowego.

Strategia, która wspiera kompetencje

Szkolenia, podcasty i poszerzanie wiedzy eksperckiej stały się naszą codziennością. W zmiennym otoczeniu uczenie się nie

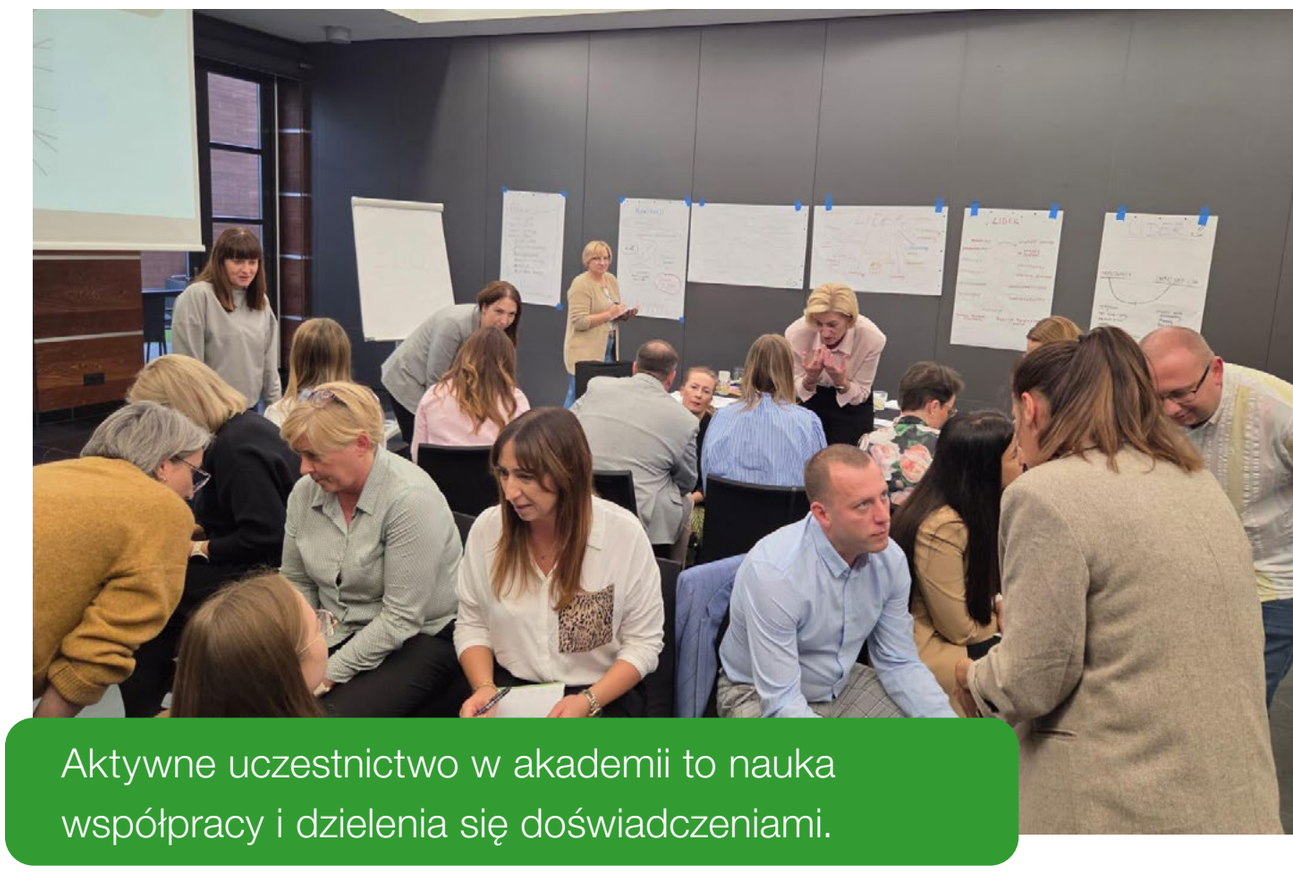
Uczestnicy Akademii Rozwoju Menadżerskiego SGB.

jest dodatkiem do pracy — stało się jej integralnym komponentem. Dlatego w aktualnej strategii SGB szczególne miejsce zajmują Centra Kompetencji, mentoring, wydarzenia zrzeszeniowe i projektowanie działań rozwojowych zgodnych z tym, jak ludzie naprawdę uczą się najskuteczniej: poprzez praktykę, doświadczenie i relację.

Wspólnie z Bankowym Ośrodkiem Doradztwa i Edukacji tworzymy inicjatywy odpowiadające realnym potrzebom Zrzeszenia. Zrealizowaliśmy już pierwsze akademie — m.in. przywództwa, personalną, menadżerską oraz Akademię Rozwoju Menadżerskiego. Każda z nich jest starannie zaprojektowana w formule blended, łącząc to, co najlepsze w szkoleniach stacjonarnych i online. Warsztaty są szyte na miarę — praktyczne, angażujące i oparte na realnych wyzwaniach uczestników.

Akademia Rozwoju Menadżerskiego to przestrzeń wymiany doświadczeń, praktycznej nauki i wspólnego poszukiwania rozwiązań – tak, by codzienne zarządzanie stawało się coraz bardziej świadome i skuteczne. W podlegającym nieustannej dynamice świecie finansów, rola menedżera to dzisiaj dużo więcej niż tylko zarządzanie procesami. Jest tu miejsce na inspirowanie zespołów, odpowiedzialne przywództwo, umiejętność podejmowania szybkich i trafnych decyzji, a także budowania kultury organizacyjnej opartej na wartościach.

Rozwój kompetencji liderskich to dziś jedno z ważnych zadań w całym sektorze, a nasza Akademia stanowi ważny proces budowania nowoczesnego przywództwa opartego na wartościach i współpracy. Wsparcie rozwoju liderów to inwestycja w przyszłość całej bankowości spółdzielczej – w jej stabilność, skuteczność i zdolność do reagowania na zmiany.



Aktywne uczestnictwo w akademii to nauka współpracy i dzielenia się doświadczeniami.

Nowe akademie: odpowiedź na przyszłe wyzwania

Nadchodzące projekty rozwojowe otworzą kolejne ścieżki w galaktyce kompetencji:

- AKADEMIA CYBERBEZPIECZEŃSTWA – by wzmocnić bezpieczeństwo danych i świadomość zagrożeń, które są dziś kluczowe dla bankowości.
- AKADEMIA GŁÓWNYCH KSIĘGOWYCH – wspierająca precyzję, odpowiedzialność i najnowsze standardy raportowania.
- AKADEMIA RELACJI BIZNESOWYCH – rozwijająca umiejętności komunikacji, budowania partnerstwa z klientem zarówno dla pracowników wspierających klienta detalicznego jak i klienta firmowego.
- AKADEMIE ROZWOJU MENADŻERSKIEGO – bo dobry lider to dziś nie tylko kierownik, ale mentor kreujący i zarządzający zmianą.

To projekty, dzięki którym pracownicy mogą rozwijać się jako specjaliści, liderzy, zyskując przewagę, która ma realny wpływ na przyszłość. ●

Co mówią uczestnicy po Akademii Rozwoju Menadżerskiego?

Ich słowa najlepiej pokazują, co naprawdę daje udział w akademiach:

„Polecamy akademię każdemu, kto jeszcze nie miał okazji wziąć udziału w tym przedsięwzięciu. Miło i produktywnie spędzony czas. Interesująca tematyka. Ogromnym plusem są zajęcia stacjonarne – dają możliwość wymiany doświadczeń i nawiązania nowych relacji. Element integracyjny to dodatkowy atut.”

Marta Banach, Anna Burchart, Ewelina Łobocka
z Banku Spółdzielczego w Czersku

„Akademia Rozwoju Menadżerskiego to miejsce, w którym teoria natychmiast zamienia się w praktykę. To nie tylko program szkoleniowy — to początek drogi pełnej rozwoju, inspirujących ludzi i nowych możliwości, które zostaną ze mną na długo. Gorąco polecam każdemu, kto chce wznieść swoje umiejętności zarządzania na wyższy poziom”

Monika Leśniak
z Banku Spółdzielczego w Dzierżoniowie

„Akademia okazała się świetną inwestycją w siebie. Praktyczne warsztaty i inspirujący prowadzący pokazują, jak budować własny, efektywny styl przywództwa. Czas spędzony na zajęciach naprawdę procentuje.”

Angelika Miotk-Rogoś
z Banku Rumia Spółdzielczego

BS

WAŻNE DLA SEKTORA

MILION RACHUNKÓW i 70 BANKÓW SPÓŁDZIELCZYCH SGB

W SYSTEMIE USŁUG SGB

Końcówka roku w Zrzeszeniu SGB upłynęła pod znakiem intensywnych wdrożeń. W trzy kolejne weekendy udało się przeprowadzić aż sześć migracji produkcyjnych banków spółdzielczych do Systemu Usług SGB. Dzięki temu SUS przekroczył symboliczny próg – już 70 Banków Spółdzielczych SGB działa w nowym systemie!

Rafał Łopka
SGB-Bank

W ostatnich tygodniach do SUS dołączyły:

- Ludowy Bank Spółdzielczy w Strzałkowie,
- Bank Spółdzielczy w Halinowie,
- Powiatowy Bank Spółdzielczy we Wrześni,
- Bank Spółdzielczy w Nasielsku,
- Bank Spółdzielczy w Osiu,
- Bank Spółdzielczy w Lubyczy Królewskiej.

Wszystkie te wdrożenia były podwójne (2 banki w jeden weekend) – łącznie w tym roku były cztery takie wdrożenia (w zeszłym roku jedno).

– System Usług SGB to wspólne (na poziomie Grupy SGB) spojrzenie na sprawozdawczość, cyberbezpieczeństwo i niezbędną automatyzacją wielu procesów. Doskonale widzimy, jak dużą rolę w cyfrowej transformacji już dzisiaj zaczyna odgrywać sztuczna inteligencja – ten cytat Szymona Paterskiego, prezesa Zarządu Powiatowego Banku Spółdzielczego we Wrześni, doskonale odzwierciedla znaczenie SUS dla całego Zrzeszenia SGB.

System Usług SGB to wspólna, zrzeszeniowa platforma technologiczno-procesowa, z której banki spółdzielcze mogą korzystać pakietowo, na zasadach subskrypcyjnych, w korzystnych dla siebie cenach. SUS zapewnia nowoczesne narzędzia, bezpieczeństwo danych, efektywność operacyjną i możliwość precyzyjnego kształtowania oferty dla klientów.

Obecnie w SUS obsługiwanych jest już milion rachunków. To dowód na rosnącą skalę i znaczenie systemu, który z miesiąca na miesiąc zyskuje nowych użytkowników.

Wdrożenia były możliwe dzięki zaangażowaniu zespołów banków spółdzielczych, SGB-Banku oraz partnera technologicznego – Asseco Poland. Współpraca, wymiana wiedzy i wspólna odpowiedzialność za projekt pozwoliły na sprawne przeprowadzenie migracji.

– Dla naszego banku decyzja o przejściu na zrzeszeniowy System Usług SGB, chociaż dojrzewaliśmy do niej powoli, ma charakter strategiczny, decydując o rozwoju naszego banku w perspektywie długoterminowej – mówi Szymon Paterski, prezes Zarządu Powiatowego Banku Spółdzielczego we Wrześni. – To projekt, na którym skorzystają przede wszystkim nasi klienci, ale również pracownicy, udziałowcy oraz lokalna społeczność. – Z punktu widzenia klienta zyskaliśmy zaawansowane technologie, cyfrowe kompetencje i nowoczesne usługi, które chcemy stopniowo wdrażać w najbliższych tygodniach, w pełni wykorzystując produkty i funkcjonalności oferowane w ramach Systemu Usług SGB, które pozwolą nam na personalizację usług dopasowując się do potrzeb

SUS przekroczył symboliczny próg – już 70 Banków Spółdzielczych SGB działa w nowym systemie!

i preferencji naszych klientów oraz podnosząc na najwyższy poziom aspekt dbałości o bezpieczeństwo powierzanych nam środków – dodaje prezes.

– Ludowy Bank Spółdzielczy w Strzałkowie zakończył proces migracji do wspólnego systemu zrzeszeniowego SUS, dołączając do grona banków korzystających z jednolitej platformy informatycznej SGB. Decyzja o wdrożeniu jest elementem strategii rozwoju, której celem jest zwiększenie bezpieczeństwa danych, unowocześnienie oferty oraz dostosowanie usług do oczekiwań klientów – mówi Dawid Majdecki, wiceprezes Zarządu Ludowego Banku Spółdzielczego w Strzałkowie.

– Migracja, realizowana przez kilka miesięcy, obejmowała szeroki zakres działań – od parametryzacji i weryfikacji danych po liczne szkolenia oraz dwie migracje testowe. W trakcie prac nasz bank wniósł także własne propozycje usprawnień projektowych, które SGB-Bank i Asseco Poland mogą wykorzystać przy kolejnych wdrożeniach, co podkreśla partnerski charakter współpracy. Dzięki zaangażowaniu wszystkich stron projekt przebiegł zgodnie z harmonogramem, a wiele etapów udało się zrealizować szybciej, niż zakładano – podkreślił wiceprezes.

A jak z perspektywy Zarządów banków wygląda weekend wdrożeniowy?

– Weekend wdrożeniowy był dla banku swoistego rodzaju testem, do którego przygotowywaliśmy się intensywnie przez okres ponad 8 miesięcy – wspomina ten moment Szymon Paterski, prezes Zarządu PBS we Wrześni. – Dziękuję pracownikom za olbrzymie zaangażowanie i pozytywne nastawienie, bez którego byłoby zdecydowanie trudniej. Wsparcie sąsiadujących z nami banków spółdzielczych, sprawna i profesjonalna współpraca i komunikacja z SGB-Bankiem i Asseco Poland, dla których komunikowane hasła „Więcej niż biznes" oraz „Technologia dla biznesu, rozwiązania dla ludzi" przekładają się na codzienne relacje partnerów i dostarczane rozwiązania.

– Przewidywaliśmy, że pierwsze dni po uruchomieniu produkcyjnym mogą wiązać się z utrudnieniami w obsłudze oraz dużą liczbą zapytań dotyczących bankowości elektronicznej i aplikacji mobilnej. Mimo intensywnej pracy, pierwsze dwa tygodnie przebiegły sprawnie, co potwierdziła również ilość i zakres zgłoszeń rejestrowanych na infolinii SGB (znacząco niższe, niż początkowo zakładano). Działania informacyjne, zwiększona dostępność i doskonałe przygotowanie pracowników przełożyły się na stabilną obsługę klientów. Cenną pomoc zapewniły również zaprzyjaźnione banki spółdzielcze, za co bardzo dziękujemy – dodaje Dawid Majdecki, wiceprezes Zarządu LBS w Strzałkowie.

> Obecnie w SUS obsługiwanych jest już milion rachunków. To dowód na rosnącą skalę i znaczenie systemu, który z miesiąca na miesiąc zyskuje nowych użytkowników.

Czas na podsumowanie wdrożeń:

– Z perspektywy kilku tygodni SUS SGB to olbrzymi projekt, duża odpowiedzialność, wielkie zaangażowanie i strategiczne spojrzenie na rozwój bankowości lokalnej opartej o najnowsze rozwiązania technologiczne. I chociaż potrzeba czasu, aby do pewnych rozwiązań i funkcjonalności się przekonać, przyzwyczaić i je dokładniej poznać to wiemy, że podjęta decyzja w kolejnych latach będzie procentować i budować relacje z naszymi klientami – przekonuje Szymon Paterski.

– Zakończenie projektu otwiera przed bankiem nowy rozdział w obszarze cyfrowej obsługi i zarządzania procesami. DEF3000 i inne narzędzia wspierające, wymagają zdobycia doświadczenia, ale dają realne możliwości usprawnienia pracy, zwiększenia automatyzacji oraz uporządkowania i podniesienia jakości danych. Zakładamy, że w dłuższej perspektywie przełoży się to na większą efektywność działania. Przyglądamy się kolejnym rozwiązaniom z katalogu usług SGB, które mogą zostać wdrożone w najbliższej przyszłości, aby dalej rozwijać ofertę i zwiększać komfort pracy i obsługi klientów – dodaje Dawid Majdecki.

> System Usług SGB będzie dalej rozwijany – w najbliższych latach planowane jest kilkadziesiąt kolejnych wdrożeń.

System Usług SGB będzie dalej rozwijany – w najbliższych latach planowane jest kilkadziesiąt kolejnych wdrożeń. Każde kolejne wdrożenie to krok w stronę nowoczesnego, zintegrowanego modelu działania bankowości spółdzielczej. ●

BS
WAŻNE DLA SEKTORA

KAPITAŁ ŻELAZNY UEP
W PRZYSZŁOŚĆ NAJLEPIEJ INWESTUJE SIĘ RAZEM

Rafał Łopka
SGB-Bank

SGB-Bank jest pierwszym partnerem Kapitału Żelaznego Uniwersytetu Ekonomicznego w Poznaniu – pierwszego takiego funduszu na publicznej uczelni w Polsce.

15 grudnia w Poznaniu bankowcy spotkali się z przedstawicielami Uniwersytetu Ekonomicznego, Fundacji UEP oraz spółki PUEB Capital w dwóch ważnych celach:

- uroczyste przekazanie środków na Kapitał Żelazny UEP,
- pierwsze spotkanie Rady Nadzorczej spółki PUEB Capital sp. z o.o. – spółka będzie zarządzać Kapitałem Żelaznym UEP.

W spotkaniu wzięli udział m.in. Mirosław Skiba – prezes Zarządu SGB-Banku, Ewelina Pałubicka – wiceprezes Zarządu SGB-Banku, prof. dr hab. Barbara Jankowska – rektor UEP i dr hab. Dawid Szutowski, prof. UEP – prorektor ds. finansów w UEP i Prezes Zarządu PUEB Capital sp. z o.o.

– Nasza współpraca z UEP to jeden z elementów Strategii SGB „Więcej niż biznes” – podkreśla Mirosław Skiba, prezes Zarządu SGB-Banku. – Dlaczego zdecydowaliśmy się na ten krok? Uważamy, że troska o polską naukę i jej przyszłość zaczyna się od stabilnych fundamentów. Kapitał żelazny pozwala inwestować środki w sposób trwały i odpowiedzialny. Tak, aby pracowały nie przez rok czy dwa, ale przez kolejne dekady, wspierając badania, stypendia, infrastrukturę i innowacyjne projekty. SGB-Bank jest pierwszym partnerem Kapitału Żelaznego UEP, ale… nie chcemy być jedyni. Zachęcamy więc wszystkich zainteresowanych (firmy, organizacje, absolwentów, liderów biznesu), a także podmioty z Klubu Partnera UEP, aby dołączyły do tego przedsięwzięcia.

Razem możemy stworzyć trwały system wsparcia, który pozwoli polskim naukowcom realizować ambitne projekty, rozwijać badania i odpowiadać na wyzwania gospodarki jutra. Będzie to miało realne przełożenie na przyszłe projekty naukowe, które mogą poprawić standard życia Polaków i przyspieszyć rozwój naszej gospodarki.

UEP to partner wiarygodny, doświadczony, działający w szerokiej, polskiej i europejskiej perspektywie, a jednocześnie bardzo mocno zakorzeniony w regionie. Z kolei Banki Spółdzielcze SGB od lat wspierają rozwój lokalnych społeczności i przedsiębiorczości w całej Polsce. Dlatego połączenie obu sił wydaje się czymś naturalnym i potrzebnym.

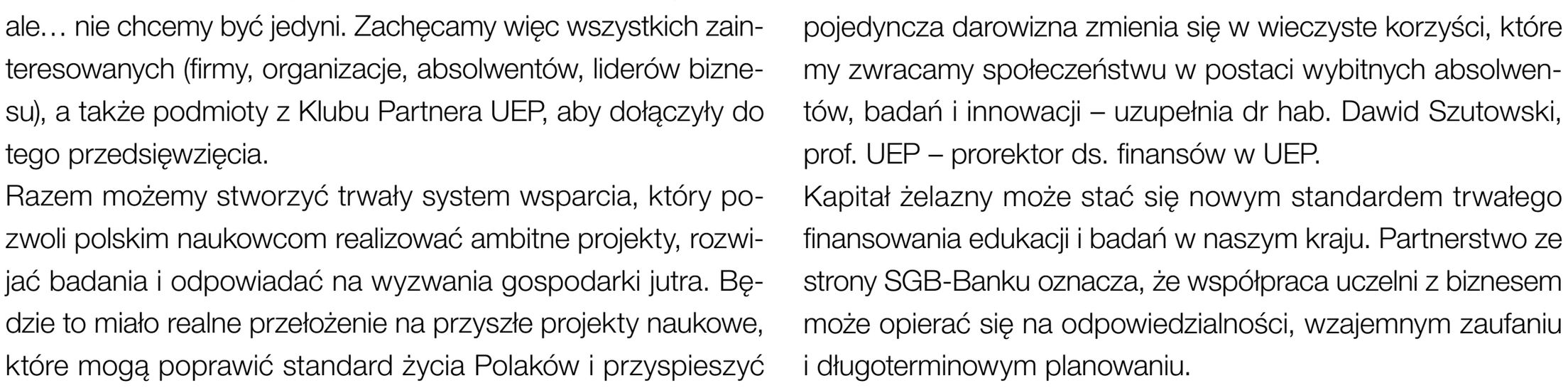
Współpraca SGB-Banku z UEP to coś więcej niż biznes.

– Kapitał Żelazny UEP to inwestycja w przyszłość Uniwersytetu Ekonomicznego w Poznaniu, która wzmacnia naszą stabilność, niezależność, możliwości rozwoju i jednocześnie pozwala nam jeszcze lepiej służyć społeczeństwu i gospodarce – wskazuje Rektor UEP, prof. dr hab. Barbara Jankowska.

– Wspólnie z partnerami biznesowymi, absolwentami i przyjaciółmi UEP budujemy trwały mechanizm rozwoju, w którym pojedyncza darowizna zmienia się w wieczyste korzyści, które my zwracamy społeczeństwu w postaci wybitnych absolwentów, badań i innowacji – uzupełnia dr hab. Dawid Szutowski, prof. UEP – prorektor ds. finansów w UEP.

Kapitał żelazny może stać się nowym standardem trwałego finansowania edukacji i badań w naszym kraju. Partnerstwo ze strony SGB-Banku oznacza, że współpraca uczelni z biznesem może opierać się na odpowiedzialności, wzajemnym zaufaniu i długoterminowym planowaniu.

Jesteśmy dumni, że wspólnie mogliśmy zrobić pierwszy krok. Teraz zapraszamy innych, aby zrobili kolejne. W przyszłość najlepiej inwestuje się razem! ●



W spotkaniu wzięli udział przedstawiciele zarówno Uniwersytetu Ekonomicznego w Poznaniu, Fundacji UEP, spółki PUEB Capital oraz SGB-Banku.

FOT. RAFAŁ ŁOPKA

BS

WAŻNE DLA SEKTORA

DLA FIRM. DLA KAŻDEGO!

TRWA KAMPANIA SGB DLA PRZEDSIĘBIORCÓW

Rafał Łopka
SGB-Bank

Czy własny biznes jest dla każdego? Czy bycie szefem jest dla każdego? Nie! Ale dla każdego, kto myśli o rozwoju swojej firmy i szuka źródeł finansowania, z całą pewnością jest oferta lokalnych Banków Spółdzielczych SGB: dostępny kredyt i tani leasing.

To główny motyw skierowanej do przedsiębiorców kampanii marketingowej Banków Spółdzielczych SGB, którą można zobaczyć w telewizji i w internecie. Jej pozytywny przekaz oparty jest na autentycznym wglądzie w rzeczywistość prowadzenia firmy i realnym wsparciu, którego lokalne banki mogą udzielić w finansowaniu bieżącej działalności oraz inwestycji. Każdy, kto myśli o rozwoju, może to zrobić wspólnie z Bankami Spółdzielczymi SGB – to podstawowy wniosek, który płynie ze spotu reklamowego przygotowanego na zlecenie SGB-Banku przez agencję GPD.

Kampania jest widoczna w telewizji (TVN, TVP), serwisach VOD (Player, TVP VOD, Polsat Go Max), a także digital – m.in. w ekosystemie Google, Meta Ads, DV360 i Onet. Dodatkowo w grudniu SGB jest obecne również na nośnikach w przestrzeni miejskiej oraz na paczkomatach w całej Polsce.

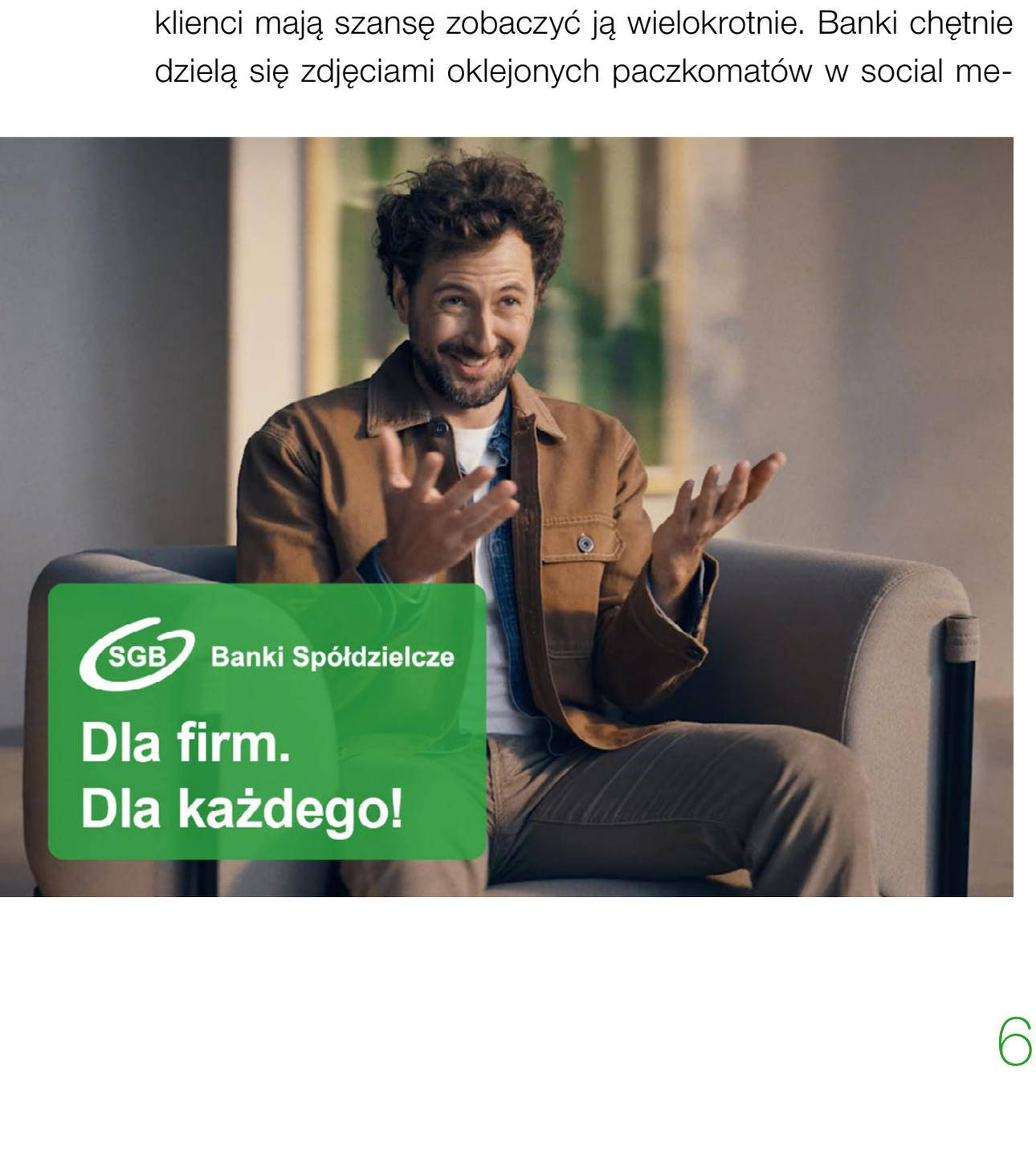
Grudniowe oklejenia paczkomatów naszą reklamą ze świątecznymi akcentami możemy już nazwać tradycją. W tym roku postawiliśmy na motyw z kampanii dla przedsiębiorców, która w grudniu jest obecna zarówno w telewizji jak i w internecie, co dodatkowo wzmocni przekaz. Na 209 maszynach, w miejscowościach, w których są Banki Spółdzielcze SGB, życzymy „Odwagi w biznesie na cały 2026 rok” razem z jedną z bohaterek aktualnego spotu. Reklama będzie wisieć cały grudzień – to czas szczególnie częstych wizyt przy paczkomatach, więc klienci mają szansę zobaczyć ją wielokrotnie. Banki chętnie dzielą się zdjęciami oklejonych paczkomatów w social mediach, a niektóre wykorzystują okazję do interakcji z klientami prosząc o zgadywanie w jakiej lokalizacji znajduje się reklama. Spotom reklamowym towarzyszy oferta kredytów i leasingu dopasowana do potrzeb firm – od finansowania środków transportu i maszyn po inwestycje w odnawialne źródła energii. Banki Spółdzielcze SGB zachęcają do współpracy przedsiębiorców z różnych branż, akcentując lokalny charakter obsługi i elastyczne podejście do finansowania biznesu.

Reklama na paczkomacie w Wieleniu.

Nowa kampania SGB opiera się na wynikach badań jakościowych i ilościowych przeprowadzonych przez SGB-Bank wśród polskich firm. Pokazały one, że 1/3 przedsiębiorców jest otwarta na korzystanie z kredytów, a jednocześnie połowa firm nie korzysta z żadnej formy kredytowania. Pozostali sięgają po usługi leasingowe i limity kredytowe w rachunkach, a kluczowe znaczenie w relacjach z bankami mają dla nich transparentność, szybkość decyzji kredytowej oraz bezpośredni kontakt z doradcą. Jednocześnie – jak wynika z badań – wielu właścicieli firm nie zdaje sobie sprawy, że Banki Spółdzielcze SGB oferują pełen zakres usług dla biznesu: od rachunków, przez leasing i ubezpieczenia, aż po finansowanie inwestycji.

– To już kolejna odsłona naszych działań marketingowych w tym roku – mówi Ewelina Ignaczak, dyrektorka Marketingu i komunikacji w SGB-Banku. – Po kampanii skierowanej do młodych klientów (#młodewilki) i kampanii kredytów hipotecznych (#hipotecznienajbliżej) zwracamy się do firm. Mamy świadomość, że przedsiębiorczość tworzy się i rozwija lokalnie – czyli tam, gdzie działają Banki Spółdzielcze SGB. To naturalni partnerzy, którzy rozumieją potrzeby przedsiębiorców i potrafią działać szybko. Wiemy, że prowadzenie własnego biznesu nie jest dla każdego, ale każdego, kto chce się rozwijać, zapraszamy do Banków Spółdzielczych SGB po produkty i usługi dopasowane do jego potrzeb i oczekiwań.

Według danych GUS w Polsce działa obecnie ponad 2,6 miliona aktywnych przedsiębiorstw, z czego zdecydowaną większość stanowią mikro – i małe firmy. To właśnie do nich kierowana jest kampania SGB – do ludzi, którzy często łączą rolę właściciela, menedżera i księgowego w jednej osobie, napędzając lokalną gospodarkę. ●



#BYCKOBIETAONTOUR

TO PROJEKT DLA KOBIET, Z KOBIETAMI, O KOBIETACH

CZERWONA TECZKA SYMBOLEM MOCY

Kończy się rok 2025. Dla projektu #byckobietaontour był to naprawdę ciekawy, intensywny i pełen pasji rok.

Marta Klepka

Projekt czerwona teczka – bo warto myśleć o rzeczach ważnych, dobrze jest o nich rozmawiać z bliskimi i nie pozostawiać spraw przypadkowi.

Spełniłam swoje marzenie! Wierzę, że z pożytkiem dla wielu kobiet. Jesteśmy przyzwyczajone do planowania strategii, budżetów, harmonogramów, ale niewiele z nas planuje i zarządza tematem, który wymaga największej odpowiedzialności – mam na myśli uporządkowanie spraw mogących okazać się kiedyś kluczowymi dla naszych bliskich. Dlatego od dawna marzyłam o tym, by przygotować dla uczestniczek konferencji #byckobietaontour czerwoną teczkę i przekonać je do jej wypełnienia.

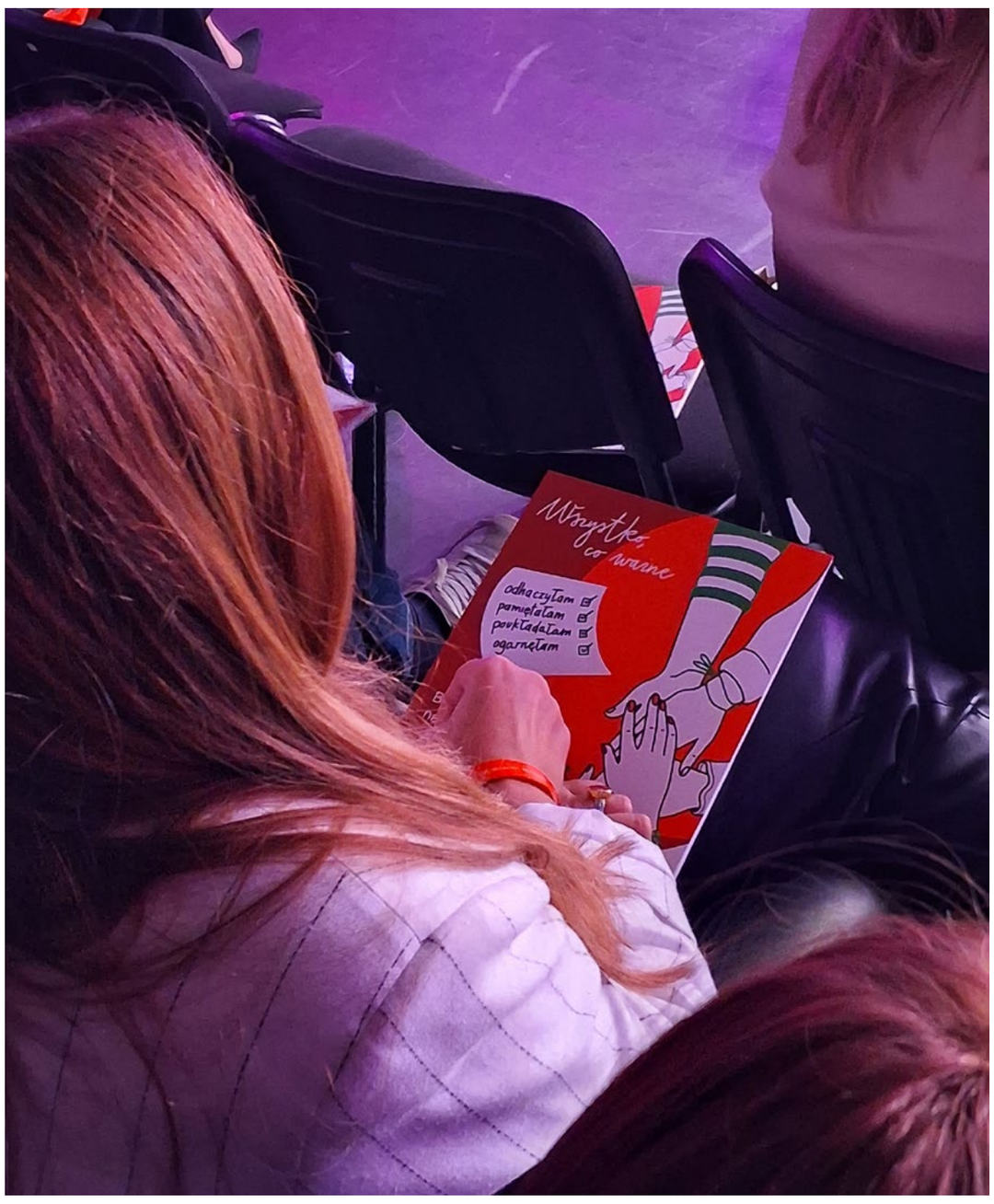
I dzięki niezwodnemu partnerowi – Bankom Spółdzielczym SGB oraz DSK Kancelarii – cenionej poznańskiej kancelarii prawno-podatkowej stało się to możliwe, za co jestem ogromnie wdzięczna.

Konferencje w całej Polsce udowodniły, że spotkanie, rozmowa i prawdziwe historie potrafią zmienić perspektywę bardziej niż niejedna książka czy wykład.

Powstała czerwona teczka, by kobiety on tour miały komplet informacji i dokumentów, które zagwarantują spokój ich rodzinom, gdy życie potoczy się inaczej, niż się spodziewają.

Zależy nam na tym, żeby kobiety zrozumiały, że wypełniona przez nie czerwona teczka daje im moc, mówi: „Jesteś ważna. To, co czujesz, ma znaczenie, Twoje życie i Twoje decyzje mają moc". Wierzymy, że uzupełniona teczka to sposób, żeby zatroszczyć się o swoich bliskich, ale także zadbać o siebie, dać sobie przestrzeń do tego, aby poukładać ważne sprawy w swoim tempie. Czerwona teczka to symbol siły i spokoju, to kontrola nad własną historią i troska na własnych zasadach o siebie i tych, których kochamy.

Podczas jesiennej edycji #byckobietaontour w Poznaniu rozmawiałam na scenie o czerwonej teczce z jej współtwórczyniami: Kingą Kozłowską-Witek – radczynią prawną i menedżerką w DSK



Kancelaria – wiodącej poznańskiej kancelarii prawno-podatkowej i Eweliną Ignaczak – dyrektorką marketingu i komunikacji w SGB-Banku. Ufam, że przekonałyśmy kobiety do tego, jak ważne jest to narzędzie. Uczestniczki konferencji znalazły czerwone teczki w swoich pakietach powitalnych i wszystkie zobowiązałyśmy się, że uzupełnimy je do kwietnia 2026 roku, czyli do kolejnej poznańskiej konferencji. Trzymam za nas kciuki!

Konferencje – #byckobietaontour łączy ludzi

Za nami 64 spotkania w 26 miastach i miasteczkach! W ciągu 8 lat w konferencjach #byckobietaontour wzięło udział już ponad 13 tysięcy uczestników, a na naszych scenach wystąpiło 170 prelegentów.

W mijającym roku w Poznaniu odbyły się dwie konferencje #byckobietaontour. Obie w Starym Browarze i obie dwudniowe: wiosenna w kwietniu i jesienna w październiku. W każdej z nich wzięło udział blisko 420 uczestniczek z całego kraju i zagranicy.

13. konferencja #byckobietaontour w Poznaniu odbyła się 4 i 5 kwietnia

I to wcale nie była pechowa edycja – wręcz przeciwnie – było mocno, prawdziwie i z silnym przekazem, że istnieje szczęśliwe „życie po…”, niezależnie od tego, z czym wcześniej przyszło się nam mierzyć. Uczestniczki wyszły z konferencji z przekonaniem, że wiara w siebie i miłość czynią cuda, a druga szansa należy się każdemu. Ważne, aby ją dobrze wykorzystać.

Tym razem postawiłam na prawdziwe, mocne historie ludzi, których życie jest dowodem, że można i że warto zawalczyć o siebie, mimo trudnego dzieciństwa, kiepskiej przeszłości, nieudanych związków, zmagania z uzależnieniami, przemocą czy bardzo poważną chorobą.

Piątkowy wieczór zostawił wszystkich z wieloma tematami do przemyśleń. Dał też moc i wiarę w to, jak wiele zależy od nas samych i od naszej otwartości na to, co podsuwa nam świat. Podczas rozmów z Ewą Gawryluk, Blanką Jordan i Zuzanną Wachowiak, Bardem Kowalskim na widowni panowało pełne skupienie. Historia Patryka Galewskiego, mimo że znana nie-

> Czerwona teczka stała się symbolem odpowiedzialności i miłości, a #byckobietaontour przestrzenią, w której kobiety uczą się dbać o siebie i swoich bliskich.

którym z filmu „Johny”, poruszyła wszystkich niezwykle mocno. Autentyczność i emocjonalność przekazu sprawiły, że trudno było opanować emocje i polały się łzy. Wieczór zwieńczyła muzyczna niespodzianka Barda Kowalskiego.

W sobotę Kamila Kalińczak we współpracy z marką Solar przekonywała, jak duży wpływ mają feminatywy na zmiany w społecznej i zawodowej sytuacji kobiet. Z wielkim entuzjazmem została przyjęta Katarzyna Grochola i jej historia. Joanna Kryńska podzieliła się swoją opowieścią o chorobie – guzie mózgu i wzmocniła wszystkich, mówiąc o sile miłości. Robert Rut-

kowski w rozmowie z Dorotą Wellman w kategoryczny i jednoznaczny sposób rozprawił się z mitami o piciu alkoholu. Nie zabrakło ważnych wykładów o zdrowiu – w trosce o serce i ciało. Nikt nie chciał, aby ten weekend się skończył…

> Zależy nam na tym, żeby kobiety zrozumiały, że wypełniona przez nie czerwona teczka daje im moc, mówi: „Jesteś ważna. To, co czujesz, ma znaczenie, Twoje życie i Twoje decyzje mają moc".

Hasłem przewodnim 14. edycji konferencji w Poznaniu była PRZYJAŹŃ

Spotkanie odbyło się 3 i 4 października. Było wartościowo i oczywiście z najlepszą energią!

O przyjaźni było naprawdę dużo – o tej prawdziwej, wspierającej, czasem cichej, ale zawsze obecnej. Było o relacjach, które dodają skrzydeł, o przyjaźni w związkach, o sile kobiecego kręgu i o tym, jak pielęgnować więzi, które są dla nas jak dom. Ważnym głosem był też głos mężczyzn i perspektywa męskiego grona prelegentów. Były wzruszenia, śmiech i prawdziwe rozmowy – dokładnie takie, jakie lubimy najbardziej. Oczywiście był i czas na refleksję.

Moje zaproszenie przyjęli naprawdę znakomici goście. Każda z tych osób wniosła swoją historię, perspektywę i moc, którą chce się dzielić. Na scenie wystąpili eksperci i prawdziwe osobowości. Byli z nami m.in.: Agata Wątróbska i Janusz Chabior, Ilona Ostrowska, Dorota Malesa, Dorota Wellman, Olga Kozierowska, Joanna Chmura, Katarzyna Przybyszewska-Ortonowska, Eryk Matuszkiewicz, Hektor Świtalski i Robert Karger.

Kolejna, 15. edycja konferencji #byckobietaontour w Starym Browarze w Poznaniu 17 i 18 kwietnia 2026 roku. Zapraszamy!

W ramach #byckobietaontour spotkałyśmy się także z setkami kobiet w kraju: w Klimkach pod Warszawą, w Łaszkowie pod Kaliszem, w Hotelu Lake Hill w Sosnówce, w My Story Gdynia Hotel, w Pałacu w Żyrowej w Opolskiem, w Lubawie na Mazurach i w innych miejscach. To są zawsze wyjątkowe, energetyczne, inspirujące wydarzenia. Cieszymy się, że tyle kobiet i mężczyzn jest z nami i razem możemy się uczyć, wzajemnie wspierać i motywować. ●

Więcej informacji:

www.facebook.com/byckobietaontour
www.instagram.com/byckobietaontour
www.byckobietaontour.pl

Marta Klepka

Jestem prawniczką, przedsiębiorczynią, ekspertką hotelarstwa, a także pomysłodawczynią, autorką i organizatorką ogólnopolskiego projektu #byckobietaontour, który tworzę głównie dla kobiet. Jestem także prowadzącą program „Babski biznes" w TVN Style.

Zarządzałam hotelami Blow Up Hall 5050 w Starym Browarze w Poznaniu i Heron Live Hotel w Gródku nad Dunajcem. Teraz zarządzam górskim hotelem Lake Hill Resort & Spa w Sosnówce w Karkonoszach. Jestem znaną i cenioną ekspertką hotelarstwa. Dzielę się swoją wiedzą i doświadczeniem podczas konferencji branżowych, a także gościnnie z widzami w programie Dzień Dobry TVN.

W ramach #byckobietaontour zorganizowałam już 64 konferencje w całej Polsce. W 2023 roku mój projekt #byckobietaontour został nagrodzony na X Polskim Kongresie Przedsiębiorczości w Krakowie.

BS
WAŻNE DLA SEKTORA

ROK SPOTKAŃ Z KLIENTAMI

RELACJE, KTÓRE BUDUJĄ BIZNES

Co jest najważniejsze w biznesie? Wiarygodność, zasady, uczciwość. Ale tego wszystkiego nie da się zbudować ani pielęgnować bez relacji. Wiem, o czym piszę, ponieważ od lat prowadzę własne wydawnictwo związane z branżą logistyczną. I wiem, jak ważne w biznesie są relacje i dobre kontakty. Banki spółdzielcze od początku istnienia na mapie finansowej Polski, swój model działania oparły właśnie na partnerskich relacjach.

Marek Loos

Mijający rok upłynął w Spółdzielczej Grupie Bankowej pod znakiem nowej strategii, nazwanej „Więcej niż biznes". Przypomnę, że strategię przyjęło Zgromadzenie Prezesów w kwietniu 2025 r. w Kołobrzegu.

Co kryje się za tym hasłem? Przede wszystkim oferowanie klientom czegoś więcej niż tylko kredytów czy lokat, ale również produktów i usług dostosowanych do potrzeb współczesnego rolnika, który jest obecnie również przedsiębiorcą. SGB stawia na bezpośrednie spotkania.

Już w pierwszych tygodniach 2025 r. tradycyjnie rozpoczęły się spotkania w Wielkopolsce, czyli tam, gdzie narodziła się bankowość spółdzielcza – w ramach „Wielkopolskich Forów Rolniczych", inaczej mówiąc, cyklu rozmów rolników z administracją państwową i samorządową. To ważna przestrzeń dialogu o polityce rolnej, opłacalności produkcji i wyzwaniach sektora.

Od lat w Forach aktywnie uczestniczy Zrzeszenie SGB, budując trwałe relacje z przedsiębiorcami rolnymi.

Dla sektora spółdzielczego współpraca z branżą AGRO pozostaje kluczowa, a szeroka oferta finansowania, zaangażowanie i udział w rynku tylko to potwierdzają. Nic dziwnego, że już kilka miesięcy później, w Warszawie, spółdzielcy z SGB zostali docenieni. Podczas tegorocznej gali Europejskiego Forum Finansowania Agrobiznesu EFFA w dniach 26–27 lutego 2025 r. po raz drugi z rzędu wyróżniono Banki Spółdzielcze SGB i SGB-Bank.

Do SGB trafiły prestiżowe nagrody Liderów Krajowego Finansowania Agrobiznesu w kategoriach:

Najlepszy Podmiot Kredytujący – SGB-Bank i zrzeszone Banki Spółdzielcze,

Najlepszy Bank Zrzeszający – SGB-Bank i zrzeszone Banki Spółdzielcze.

Naszą walutą jest czas

Jak powiedział mi jeden z prezesów: „Naszą przewagą jest fakt, że potrafimy słuchać klientów i mamy dla nich bezcenną walutę. Tą walutą jest czas. Zawsze znajdujemy czas dla naszych klientów".

Tak było w Warszawie i nie inaczej było w Bednarach pod Poznaniem, gdzie SGB wspólnie z SGB Leasing zaprosili klientów

Podczas I Regionalnego Forum Gospodarczego w Jarocinie nie mogło zabraknąć ekspertów z lokalnego banku, których wspierali pracownicy SGB-Banku.

do swojego pawilonu na największych targach rolniczych w Europie. To wyjątkowe wydarzenie, które od lat cieszy się ogromnym zainteresowaniem zarówno profesjonalistów, jak i osób prywatnych. To doskonałe miejsce prezentacji najnowszych rozwiązań rolniczych, ale także rozmów o trendach w rolnictwie, transformacji energetycznej i zielonej gospodarce. I tutaj również mocny głos należy do polskiego sektora bankowości spółdzielczej.

Banki spółdzielcze od początku istnienia swój model działania oparły właśnie na partnerskich relacjach.

Zielona Perspektywa SGB – realne wsparcie dla przedsiębiorców

Banki Spółdzielcze SGB coraz mocniej angażują się w rozwój lokalnej energetyki oraz zielonej transformacji biznesu. Doskonałym przykładem były konferencje organizowane w regionach,

Konferencja zorganizowana pod koniec listopada w Urzędzie Marszałkowskim w Poznaniu. Na pytania uczestników dotyczące pozyskiwania środków z funduszy unijnych odpowiadali eksperci z banku zrzeszającego.

podczas których przedsiębiorcy mogli poznać konkretne możliwości inwestowania w odnawialne źródła energii.

W marcu w Ostrowie Wielkopolskim – dzięki współpracy BS w Dobrzycy, Jarocinie, Raszkowie, SBL Skalmierzyce oraz SGB-Banku – uczestnicy rozmawiali o finansowaniu projektów OZE, nowych technologiach oraz usługach wspierających rozwój biznesu, takich jak leasing czy faktoring. Ważnym punktem spotkania był panel o cyberbezpieczeństwie, przypominający, jak chronić firmowe finanse w dynamicznie zmieniającym się otoczeniu zagrożeń.

Podobny charakter miało wydarzenie w Pleszewie, przygotowane przez tamtejszy bank spółdzielczy we współpracy z bankami regionu. Głównym tematem stały się możliwości rozwoju biogazowni i lokalnych spółdzielni energetycznych. Eksperci podkreślali, że choć w Niemczech działają tysiące instalacji biogazowych, w Polsce rozwój tego sektora dopiero nabiera tempa. To ogromna szansa – zarówno dla środowiska, jak i lokalnych przedsiębiorców, którzy dzięki takim inwestycjom mogą obniżyć koszty energii, zwiększyć niezależność i tworzyć nowe miejsca pracy.

Oba wydarzenia doskonale wpisują się w program Zielona Perspektywa SGB – strategiczną inicjatywę Grupy, której celem jest zwiększenie udziału Banków Spółdzielczych SGB w finansowaniu projektów związanych z zieloną transformacją. To nie tylko oferta kredytowa, lecz także wsparcie edukacyjne, współpraca z partnerami technologicznymi i budowanie lokalnej współpracy.

SGB coraz mocniej angażuje się w rozwój lokalnej energetyki oraz zielonej transformacji.

Inwestycje w przyszłość

W tym duchu utrzymane było I Regionalne Forum Gospodarcze „Inwestycje Przyszłości Jarocin 2025”, gdzie ponownie podkreślono znaczenie Zielonej Perspektywy SGB. W debacie o zielonej gospodarce Jan Grzesiek, prezes BS w Jarocinie i przewodniczący Rady Nadzorczej SGB-Banku, zaznaczył: „Oferujemy przedsiębiorcom korzystne rozwiązania finansowe, które pozwalają obniżyć koszty energii i uniezależnić się od wahań cen prądu. Nasza oferta sprawia, że nowoczesne technologie energetyczne stają się realne nawet dla małych i średnich firm”. Wskazał również na rosnące zainteresowanie Pożyczką OZE rozwijaną wspólnie z BGK i Funduszami Europejskimi.

Spotkania z przedsiębiorcami (nie sposób wymienić wszystkich) odbyły się też w Poznaniu. Konferencja zorganizowana w Urzędzie Marszałkowskim potwierdziła, że zielona transformacja staje się dla wielkopolskich firm realnym kierunkiem rozwoju. Sporym zainteresowaniem cieszyła się Pożyczka OZE, o której szczegółowo opowiadali eksperci z SGB-Banku.

Liczne pytania przedsiębiorców pokazały, że poszukują oni konkretnych, dostępnych narzędzi wspierających inwestycje w OZE. Spotkanie udowodniło, że zielone inwestycje przestają być hasłem, a stają się praktycznym wyborem biznesu.

Relacje były, są i będą fundamentem spółdzielczości. A przyszłość – zielona, odpowiedzialna i oparta na współpracy – tworzy się właśnie tam, gdzie ludzie potrafią ze sobą rozmawiać. I dlatego Banki Spółdzielcze SGB mają dziś więcej niż przewagę. Mają rolę do odegrania. ●

Fora Rolnicze to cykl spotkań, które w pierwszej połowie roku organizuje Wielkopolska Izba Rolnicza. Zawsze obecne są Banki Spółdzielcze SGB. Na zdjęciu pracownicy Banku Spółdzielczego w Koninie.

Osobista refleksja autora

Przyglądając się tym wszystkim wydarzeniom, mam wrażenie, że wracamy do źródeł. Do idei spółdzielczości, która zawsze opierała się na wspólnocie, odpowiedzialności i działaniu dla dobra lokalnych społeczności. W czasach globalnych kryzysów energetycznych i niepewności gospodarczej te wartości nabierają nowego znaczenia. I może właśnie dlatego bankowość spółdzielcza przeżywa dziś swój renesans – bo oferuje coś, czego nie da się skopiować ani zastąpić algorytmem: **relację z człowiekiem.**

BANKOWOŚĆ BEZ BARIER

– W JAKI SPOSÓB WSPIERAĆ OSOBY ZE SZCZEGÓLNYMI POTRZEBAMI?

Adam Karmoliński

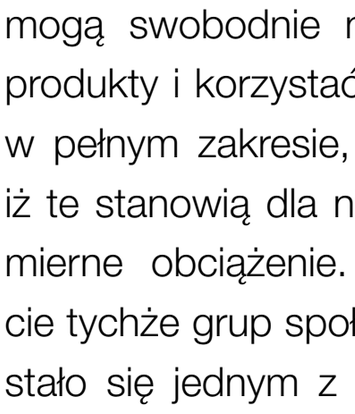
Jan Solarski

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

Od początku XXI w. w polskim społeczeństwie rośnie świadomość i zainteresowanie potrzebami osób z niepełnosprawnościami. Coraz wyraźniej dostrzega się, iż w razie odpowiedniego dostosowania otoczenia, osoby te mogą aktywnie uczestniczyć w życiu społecznym i funkcjonować na równi z innymi obywatelami. Jednocześnie, dynamiczne zmiany cywilizacyjne, rozwój usług cyfrowych i przenoszenie wielu aktywności do Internetu uświadomiło, iż niepełnosprawność fizyczna czy umysłowa stanowi tylko jedną z barier utrudniających codzienne funkcjonowanie. Okazało się, że wyzwania związane z dostępnością mogą ograniczać również ludzi w pełni sprawnych, którzy ze względu na swój wiek, stan zdrowia, miejsce zamieszkania czy obowiązki rodzicielskie nie zawsze mogą swobodnie nabywać produkty i korzystać z usług w pełnym zakresie, a bywa iż te stanowią dla nich nadmierne obciążenie. Wsparcie tychże grup społecznych stało się jednym z priorytetów zarówno państw członkowskich Unii Europejskiej, jak również samej Wspólnoty.

> Inną grupą odbiorców mogącą cieszyć się z wprowadzanych rozwiązań są seniorzy.

Przykładem działań w tym kierunku jest nowo wprowadzana ustawa, która wedle założeń ma ograniczać istniejące bariery oraz zobowiązywać przedsiębiorców do pełniejszego uwzględniania potrzeb osób o szczególnych wymaganiach. Mowa o *ustawie z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze* (dalej: „Ustawa"). Jest ona rezultatem implementacji do polskiego porządku prawnego przepisów *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług,* zwanej dalej „Dyrektywą 2019/882". Głównym celem Dyrektywy 2019/882 jest ujednolicenie wymogów dostępności wybranych produktów i usług, aby zapewnić sprawniejsze funkcjonowanie rynku wewnętrznego UE poprzez eliminowanie i zapobieganie barierom wynikającym z rozbieżnych przepisów krajowych. Jest to pierwszy tak szeroko regulujący akt prawa unijnego, który ma zapewnić, że podmioty gospodarcze oraz administracja publiczna będą stosować jednolite zasady dostępności wybranych produktów i usług (w tym produktów i usług bankowych), przyczyniając się tym samym do realizacji celów oraz założeń Europejskiej Strategii w sprawie niepełnosprawności. To niezwykle ważne dla osób niepełnosprawnych, których wedle treści uzasadnienia projektu Ustawy, mieszka w Polsce między 4,9 a 7,7 mln[1].



Inną grupą odbiorców mogącą cieszyć się z wprowadzanych rozwiązań są seniorzy, którzy bazując na pogarszających się prognozach demograficznych dla naszego kraju, będą stanowili coraz liczniejszą grupę społeczną, podatną zarazem na różnego rodzaju wykluczenia i ograniczenia. Wydaje się, iż oprócz ograniczeń zdrowotnych, najtrudniejsze do przezwyciężenia będą dla nich ograniczenia cyfrowe, szczególnie dla osób powyżej 80. roku życia, których liczba w 2030 r. ma przekroczyć 2 mln osób[2]. Wraz z upływem czasu liczba

1 Inne dane opublikował Główny Urząd Statystyczny, który w raporcie na dzień 31 grudnia 2024 r. wskazał, iż Polskę zamieszkuje 3,9 miliona osób posiadających ważne orzeczenie o niepełnosprawności (https://stat.gov.pl/obszary-tematyczne/warunki-zycia/ubostwo-pomoc-spoleczna/osoby-niepelnosprawne-w-2024-r-,26,7.html [dostęp na dzień 24.11.2025 r.]).

2 Główny Urząd Statystyczny, Sytuacja demograficzna osób starszych i konsekwencje starzenia się ludności Polski w świetle prognozy na lata 2014–2050, Warszawa 2014 (https://stat.gov.pl/obszary-tematyczne/ludnosc/

ta będzie tylko i wyłącznie rosła, co bez wątpienia doprowadzi do dalszego wzrostu liczby obywateli wymagających szczególnej uwagi.

Zrozumiałość i kompatybilność metod identyfikacji konsumenta

Przechodząc jednak do Ustawy, zgodnie z jej założeniami (art. 16) świadczenie usług bankowości detalicznej powinno spełniać kryteria dostępności, postrzegalności, funkcjonalności, zrozumiałości i kompatybilności metod identyfikacji konsumenta, składania podpisów elektronicznych, bezpieczeństwa usług płatniczych. Natomiast wszelkie przekazywane klientom informacje powinny być komunikowane w języku polskim, bądź za zgodą konsumenta w innym języku na poziomie biegłości językowej B2. Ponadto, komunikaty kierowane do klienta należy w miarę możliwości przekazywać za pomocą więcej niż jednego kanału sensorycznego, w sposób zapewniający ich zrozumiałość, w formatach tekstowych umożliwiających wykorzystanie ich w alternatywnej komunikacji, czy też przy pomocy odpowiedniej czcionki. Każdorazowo powinna być zapewniona pewna alternatywa umożliwiająca osobom o szczególnych potrzebach skorzystanie z określonych produktów oraz usług, w tym np.

- w przypadku komunikowania się – dostęp do rozwiązań umożliwiających komunikację wizualną, dźwiękową, za pośrednictwem mowy oraz dotyku;
- w przypadku wykorzystywania koloru do przekazywania informacji – dostęp do rozwiązań alternatywnych do stosowania kolorów;
- w przypadku wykorzystywania mowy – dostęp do funkcjonalności umożliwiających alternatywną do mowy komunikację, wprowadzanie danych głosowych na potrzeby komunikacji;
- w przypadku wykorzystania elementów wizualnych – zapewnienie wyrazistości wizji oraz rozwiązań umożliwiających powiększenie obrazu, zwiększenie jego jasności i kontrastu czy interoperacyjność z narzędziami wspomagającymi.

Dlaczego wprowadzanie nowych rozwiązań legislacyjnych w tym zakresie było konieczne? Pomimo, iż regułą jest, że bankom opłaca się rozszerzać swoją ofertę i kierować swoje usługi do nowych grup odbiorców, osoby ze szczególnymi potrzebami nadal wydają się niedostatecznie dostrzegane. Następujące wnioski można wyciągnąć m.in. z raportu „Dostępność produktów i usług bankowości detalicznej dla osób ze szczególnymi potrzebami w Polsce" opublikowanego w maju 2025 r. na stronie Rzecznika Finansowego[3]. Z treści raportu sporządzonego przy wsparciu pracowników Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego można wyciągnąć druzgocące wnioski. Mianowicie, do czasu wydania raportu zaledwie około 5% podmiotów zadeklarowało, iż przeszkolonych z zakresu dostępności jest większość pracowników placówek. Ponad 80% udzielonych odpowiedzi sygnalizowało zupełny brak przeszkolenia pracowników. Podobnie prezentowały się odpowiedzi na pytanie w ilu procentach placówek pracuje przynajmniej jeden przeszkolony pracownik. Sektor bankowy zdecydowanie lepiej oceniał zrozumiałość przedkładanych klientom materiałów, wyświetlanych treści w Internecie czy dostępność nakładek/dokumentów w alfabecie Braille'a, natomiast zdecydowanie gorzej wypadła dostępność pętli indukcyjnych w placówkach banku czy dostępność placówek, w których można porozumieć się w języku migowym.

> Komunikaty kierowane do klienta należy przekazywać za pomocą więcej niż jednego kanału sensorycznego.

Zmiany na stronach www i w aplikacjach bankowych

W jaki sposób na wymogi ustawowe zareagowały polskie banki? Zmiany widoczne są przede wszystkim na stronach internetowych i w aplikacjach bankowych. Część z banków postanowiło zwiększyć kontrast prezentowanych klientom treści ułatwiając dostęp do swoich usług osobom z wadami wzroku czy chorobami oczu. Strony internetowe banków zostały wyposażone również w wirtualnych asystentów, którzy mogą komunikować się z nami zarówno pisemnie, jak i głosowo. Innym rozwiązaniem wspierającym osoby głuchonieme jest wprowadzenie infolinii z językiem migowym. Oczywiście, w ich przypadku komunikacja będzie odbywać się za pośrednictwem rozmowy audio-wideo, z naciskiem na komunikację przy pomocy ruchów oraz gestów ciała. Niemniej jednak, taki rodzaj komunikacji umożliwiający skorzystanie z więcej niż jednego kanału sensorycznego, może ułatwić komunikację z klientami o innych wymogach. Pewne zmiany można zauważyć również w dokumentacji oraz komunikatach marketingowych. Postawiono w nim nacisk na prosty język, który będzie zrozumiały dla zwykłego klienta. Oczywiście, część banków unowocześniła również swoje placówki doposażając je w pętle indukcyjne, lupy oraz ramki do podpisu. Umożliwiono ponadto wejście z psem przewodnikiem czy w części lokali ułatwiono dostęp dla osób poruszających się na wózku czy rodziców z dziećmi.

> W komunikatach marketingowych postawiono nacisk na prosty język, który będzie zrozumiały dla zwykłego klienta.

W obliczu coraz szybszego rozwoju technologicznego oraz stopniowego poszerzania się grona osób o szczególnych potrzebach, z zadowoleniem należy spojrzeć na kierunek zmian, do których dochodzi w polskiej bankowości. Oczywiście, część zmian wymuszana jest zmianami legislacyjnymi, za którymi stoją europejskie oraz polskie władze prawodawcze. Niemniej jednak, banki coraz częściej same postanawiają wyjść do klientów usuwając piętrzące się przed nimi ograniczenia czy informując o czyhających na nich zagrożeniach w świecie wirtualnym. Mamy nadzieję, iż dostosowywanie metod świadczenia usług do potrzeb i zdolności klientów pójdzie jeszcze dalej ku strategiom opierającym się na klientocentryczności. ●

ludnosc/sytuacja-demograficzna-osob-starszych-i-konsekwencje-starzenia-sie-ludnosci-polski-w-swietle-prognozy-na-lata-2014-2050,18,1.html [dostęp na dzień 24.11.2025 r.]).

3 https://rf.gov.pl/wp-content/uploads/2025/05/Raport-final-1.pdf (dostęp na dzień 24.11.2025 r.).

TROCHĘ KULTURY

Yuval Noah Harari „Nexus. Krótka historia informacji od epoki kamienia do sztucznej inteligencji”. Na język polski przełożył Justyn Hunia.

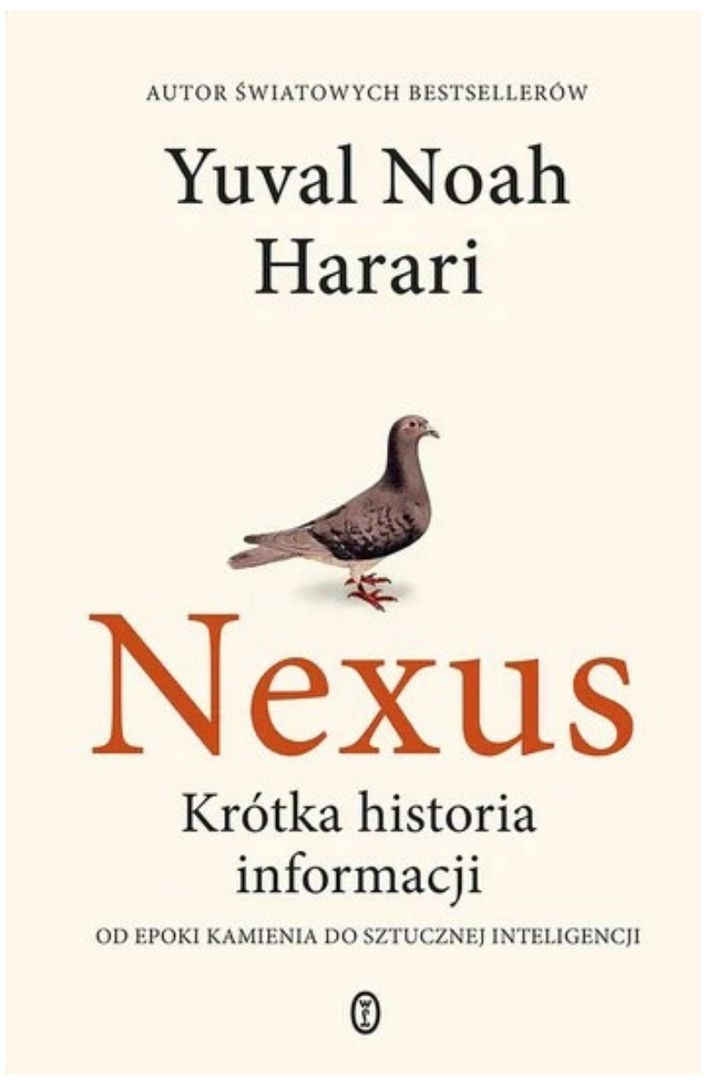
RAFAŁ ŁOPKA, SGB-BANK

Yuval Noah Harari to izraelski historyk, profesor historii na Uniwersytecie Hebrajskim w Jerozolimie, autor bestsellerów: „Sapiens. Od zwierząt do bogów”, „Homo Deus. Krótka historia jutra” i „21 lekcji na XXI wiek”, które na nowo zdefiniowały popularne spojrzenie na dzieje ludzkości i jej przyszłość.

Jego monumentalne dzieło „Sapiens” w genialny, zwarty i dowcipny sposób przedstawiło syntetyczną historię naszego gatunku. Harari przeanalizował kluczowe rewolucje, dowodząc, że to umiejętność współistnienia w ramach wspólnych mitów umożliwiła masową współpracę i panowanie nad światem. Mój ulubiony bon-mot z książki: największym wygranym w historii ludzkości jest… kukurydza, która z regionalnego warzywa w Ameryce Południowej stała się globalnie uprawianą rośliną.

Następnie, w „Homo Deus”, Harari skupił się na przyszłości. Przedstawiał wizje zagrożeń związanych z dominacją sztucznej inteligencji, biotechnologią i dążeniem człowieka do „boskości”. Przerażające jest to, że po kilku latach część przewidywań sprawdziła się co do joty, a w niektórych przypadkach rzeczywistość przekroczyła jego wyobrażenia.

Harari od lat podkreśla globalny charakter wyzwań. Podczas poznańskiej konferencji Impact’22 zwrócił uwagę, że choć żyjemy w „złotym wieku” pod względem dostępu do zdrowia i edukacji, to wiele współczesnych kryzysów (od pandemii po agresję Rosji na Ukrainę) – wynika z erozji liberalnego porządku światowego i braku prawdziwej globalnej współpracy.



„Nexus” stanowi logiczną kontynuację wcześniejszych prac, ale oferuje nową perspektywę: zamiast patrzeć wyłącznie wstecz (Sapiens) lub w przyszłość (Homo Deus), książka zagłębia się w proces tego, jak idee, narracje i algorytmy kształtują nasz świat.

Najnowsza książka Hararyego analizuje historię sieci informacyjnych człowieka. Od prymitywnych wierzeń i mitów, poprzez rozwój dokumentów, druku, mediów masowych, aż po erę sztucznej inteligencji. Harari stawia fundamentalne pytania o naturę informacji, jej rolę w tworzeniu porządku i znaczenia oraz o przyszłość, gdy to nie człowiek, ale maszyna będzie kreować rzeczywistość.

Książka łączy retrospekcję (znów wracamy do początku naszego gatunku) z analizą teraźniejszości, zwłaszcza roli AI w sieciach informacyjnych. Nie zabrakło ciekawych, konkretnych przykładów, takich jak Rzym czasów cesarzy, Palestyna na przełomie er, aż po totalitaryzmy Stalina czy Hitlera. Odpowiada też na wiele pytań:

- Jak informacje łączą ludzi, ale też jak rozpowszechniają fake newsy. Spojler: kiedyś nazywane propagandą.
- W jaki sposób demokracja umożliwia naprawę własnych niedoskonałości, podczas gdy autorytaryzm stara się je zamrozić (z różnymi konsekwencjami).
- Czy sztuczna inteligencja nie tylko zbiera dane, ale zaczyna tworzyć narracje. Byłby to pierwszy raz w historii ludzkości, gdy „sieć” może działać niezależnie od nas.
- Czy AI może wzmacniać uprzedzenia, a „czarne skrzynki” algorytmów mogą podważać naszą autonomię i demokrację?

Jak zawsze, Harari otacza swoją opowieść ogromnym kontekstem historycznym (skąd wzięła się nazwa Tel Awiw, kto napisał „Młot na czarownice”?) i łączy go z refleksją na temat współczesności, oferując czytelnikowi spójny sposób na porządkowanie złożoności świata.

Oczywiście Harari ma tez swoje wady: czasem upraszcza pewne zagadnienia, czasem mocno dostosowuje argumenty do stawianych przez siebie tez, zdarza mu się też pomijać kluczowe kultury, np. Indie. Martwi też jego alarmistyczne podejście do AI, ale któż z nas nie oglądał „Terminatora”?

„Nexus”, choć momentami jest książką przewidywalną, w ciekawy sposób porządkuje transformację informacyjną, zarówno historyczną, jak i teraźniejszą. Główna teza wybrzmiewająca po lekturze jest potężna: to informacja od zawsze była siłą zdolną zarówno do budowania, jak i do niszczenia cywilizacji. Jeśli masz rozpocząć przygodę z tym autorem, zacznij od „Sapiens”. Jeśli jesteś fanem Hararyego, przeczytasz „Nexus” z przyjemnością, zgodnie z zasadą, że najbardziej lubimy te utwory, które znamy. ●

Wczasy – Dżungla

JĘDRZEJ SZYMANOWSKI, SGB-BANK

Koniec roku to czas podsumowań, wspominania zdarzeń, osób, emocji. Zamykamy w ten sposób ostatnie 12 miesięcy, ale nierzadko okres ten sprzyja poszerzaniu tej refleksji i wybieganiu jeszcze dalej w przeszłość. Rekapitulacja dotychczasowych dokonań pozwala się zresetować i przyjąć nową perspektywę na przyszłość. Odsłuch nowej płyty Wczasów niesie sugestię, że podobne myśli towarzyszyły zespołowi podczas jej tworzenia.

Poznański duet od prawie dekady działa na alternatywnej scenie, czego efektami są trzy płyty, jedna EP-ka i niezliczona liczba koncertów, na których niezmiennie bawią publiczność swoim niewymuszonym luzem. Czysto muzycznie, ich piosenki zgrabnie manewrują między zimną falą i wesołym indie rockiem. W tekstach zaś potrafią zręcznie oddać niepokoje życia we współczesnej Polsce – pokrzepiająco i z humorem, bez popadania w defetyzm i coachingową demagogię. Bo

bohaterowie Wczasów – choć przejmuje ich skomplikowana sytuacja geopolityczna, korporacyjny wyścig, życie w kapitalistycznym potrzasku, patodeweloperka i katastrofa klimatyczna – podchodzą do tych zagrożeń ze zgryźliwą, ale żartobliwą ironią. Cechuje ich samoakceptacja i chęć pozytywnego spojrzenia na każdą, nawet najbardziej beznadziejną sytuację. Na nowym albumie słychać to nawet bardziej niż wcześniej.

Poprzednia płyta Bartka i Kuby, „To wszystko kiedyś minie" z 2021 roku, choć nadal była wydawnictwem alternatywnym, nosiła znamiona dopracowanego, ambitnego przedsięwzięcia. Premierę przekładali ze względu na okres covidowy, kiedy nie można było grać promujących materiał koncertów. Ten sprzyjał z kolei cyzelowaniu szczegółów. Po tak wyczerpujących pracach produkcyjnych, przy okazji kolejnego albumu chłopaki postawili na zmianę podejścia. „Dżunglę" wypełniają zwarte, bezpretensjonalne piosenki, nagrane i zrealizowane sprawnie, bez rozczulania się nad detalami. Wczasy pokazują na niej wszystko to, co autentycznie lubią – bez żadnego udawania i niepotrzebnie ciążącej ambicji. Koresponduje to z tekstami, z których przebija pochwała skromnego, spokojnego życia. W kilku piosenkach przewija się opozycja Poznań-Warszawa, jako symboliczna konfrontacja równowagi i niezdrowych aspiracji. Wczasy pokazują, że uparte dążenie do perfekcji nie zawsze jest zdrowe – lepiej doceniać to, co mamy i co potrafimy. I cieszyć się tym w pełni. Warto zastanowić się nad takim podejściem do życia przy okazji wchodzenia w nowy rok. ●

BS

Wydarzenia w SGB 2025

Styczeń

Trwa kampania Młode Wilki
Pokazywaliśmy w niej, że cenimy i lubimy młodych ludzi.
I że wspieramy ich w ich wyborach.

SGB Banki Spółdzielcze | Dobrze dbać o siebie nawzajem

Otwórz konto dla #MłodychWilków

Sprawdź

Luty

Nagrody dla rolnictwa EFFA

Banki Spółdzielcze SGB są liderami finansowania rolnictwa w Polsce. Podczas gali Europejskiego Forum Finansowania Agrobiznesu EFFA 2025 doceniono ten fakt licznymi statuetkami.

Marzec

Kredyty konsorcjonalne dla spółek SGB Faktoring i SGB Leasing.

Konsorcjum składające się z 28 Banków Spółdzielczych SGB oraz SGB-Banku podpisało umowę kredytu konsorcjalnego ze spółką SGB Faktoring SA. Łączna kwota umowy to 100 mln zł.
93 Banki Spółdzielcze SGB oraz SGB-Bank stworzyły konsorcjum kredytowe, które sfinansuje rozwój spółki SGB Leasing. Wartość umowy to 200 mln złotych.

Kwiecień

SGB z nową strategią **„Więcej niż biznes”**
Zgromadzenie Prezesów Banków Spółdzielczych SGB przyjęło nową strategię Spółdzielczej Grupy Bankowej na lata 2025-2028. Dokument z hasłem „Więcej niż biznes” koncentruje się na dwóch filarach: rozwoju biznesu i zwiększaniu sprawności operacyjnej.

Maj

Wystartowało
WYZWANIE SPORTOWE SGB

W tegorocznej edycji Wyzwania Sportowego SGB bankowcy z Grupy SGB, partnerzy z współpracujących z nami instytucji, ale przede wszystkim sympatycy SGB przez 44 dni zbierali kilometry w szczytnym celu. W tym roku pobiliśmy rekord uczestników (9 tysięcy) i rekord sympatyków SGB (blisko 5,2 tysiąca osób). Łącznie pokonaliśmy na nogach i kołach ponad 2,5 miliona kilometrów!

Czerwiec

Walne Zgromadzenie Akcjonariuszy SGB-Banku i wybór nowej Rady Nadzorczej SGB-Banku

W Poznaniu odbyło się Walne Zgromadzenie Akcjonariuszy SGB-Banku, które udzieliło absolutorium za 2024 rok członkom Rady Nadzorczej i Zarządu. Akcjonariusze dokonali również wyboru członków Rady Nadzorczej SGB-Banku na nową kadencję w latach 2025-2028.

Lipiec

Uniwersytet Ekonomiczny w Poznaniu i SGB-Bank budują kapitał dla nauki.Uniwersytet Ekonomiczny w Poznaniu stał się pierwszą publiczną uczelnią z kapitałem żelaznym w Polsce. UEP podpisał umowę na kapitał żelazny z pierwszym partnerem, którym jest SGB-Bank.

Wrzesień

Jubileusz 35-lecia SGB-Banku i **SGB** oraz **wybór nowej Rady Zrzeszenia SGB**

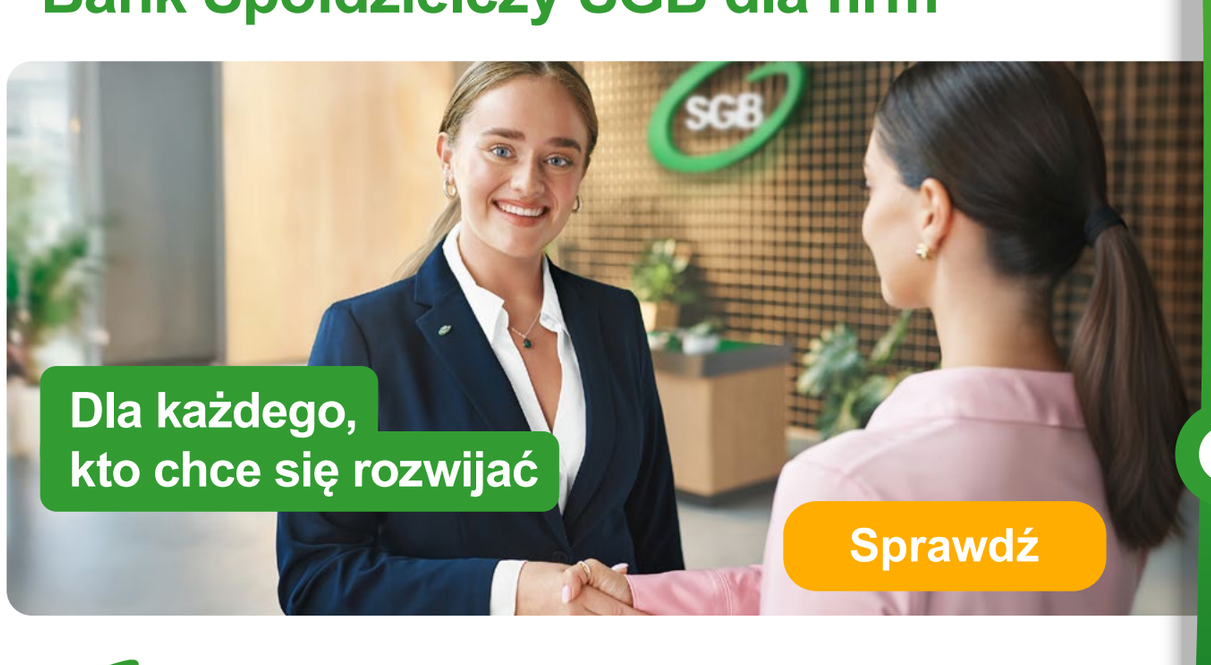
W Poznaniu obradowało Zgromadzenie Prezesów Spółdzielczej Grupy Bankowej, które dokonało wyboru nowej Rady Zrzeszenia i oceniło efekty działań ostatniego półrocza. W salach Międzynarodowych Targów Poznańskich SGB-Bank i SGB obchodzili jubileusz 35-lecia działalności. To było święto całej Spółdzielczej Grupy Bankowej.

Listopad

Ruszyła kampania marketingowa Banków Spółdzielczych SGB skierowana do przedsiębiorców

Dla firm. Dla każdego! – to główny motyw skierowanej do przedsiębiorców kampanii marketingowej Banków Spółdzielczych SGB. Każdy, kto ma firmę i myśli o jej rozwoju, może to zrobić wspólnie z Bankami Spółdzielczymi SGB.

Bank Spółdzielczy SGB dla firm



SGB Bank Spółdzielczy | **Dla firm. Dla każdego!**

70 Banków w SUS

System Usług SGB przekroczył symboliczny próg – jest w nim już 70 Banków Spółdzielczych SGB. Obecnie w SUS obsługiwanych jest już milion rachunków, to blisko połowa wszystkich rachunków w Zrzeszeniu SGB.

Sierpień

Wystartowała kampania kredytu hipotecznego

Ruszyła kolejna kampania reklamowa Banków Spółdzielczych SGB „Hipotecznie najbliżej”. Promowaliśmy w niej kredyty hipoteczne na „swoje miejsce”.

SGB Banki Spółdzielcze — Hipotecznie najbliżej

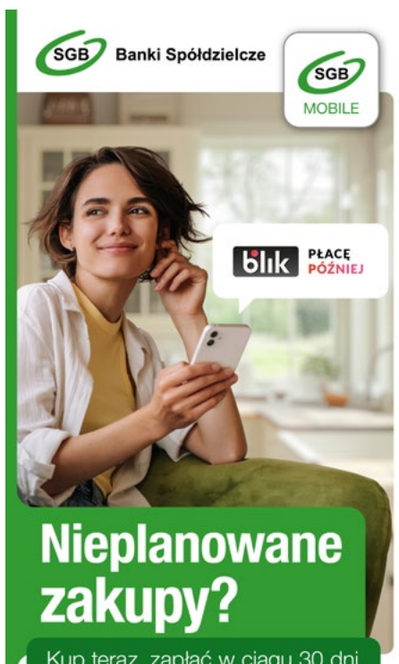
Październik

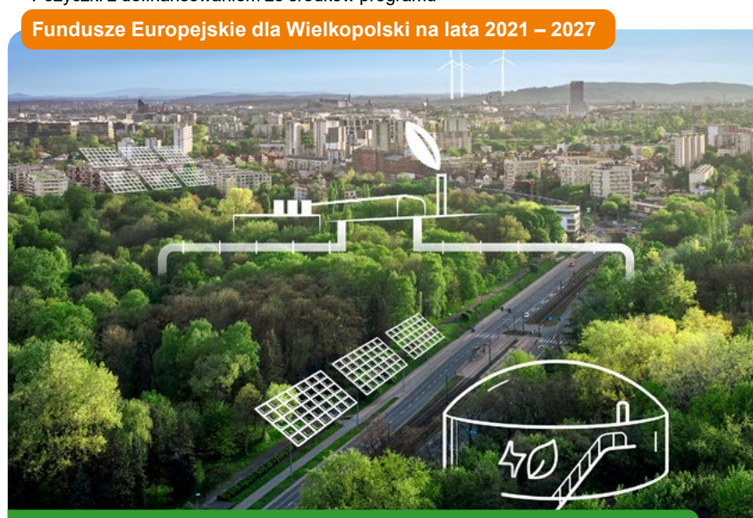
Blik płacę później

Banki Spółdzielcze SGB, jako jedne z pierwszych w Polsce, uruchomiły usługę BLIK Płacę Później, dzięki której można zrobić zakupy online i zapłacić za nie nawet do 30 dni później, bez dodatkowych kosztów.

Pożyczki OZE

SGB-Bank podpisał z Bankiem Gospodarstwa Krajowego Umowę Operacyjną Instrument Finansowy – Pożyczka na OZE z dotacją w formie umorzenia dla instytucji z województw wielkopolskiego i łódzkiego.





Grudzień

100 banków w SOC, BLIK Płacę Później i Wielowalutowości

Ponad 100 Banków Spółdzielczych SGB korzysta z nowoczesnych usług przygotowanych przez SGB-Bank. Nasza strategia „Więcej niż biznes” to zobowiązanie do tworzenia ekosystemu usług, który wspiera banki spółdzielcze w rozwoju, zwiększa ich konkurencyjność i zapewnia bezpieczeństwo klientom. Dzisiaj w tym ekosystemie kluczową rolę odgrywają trzy usługi: SOC SGB, BLIK Płacę Później – BNPL oraz Wielowalutowość.

BODiE
Grupa SGB

WIEDZA
EDUKACJA
ROZWÓJ

Zapraszamy na stacjonarne szkolenia organizowane w Poznaniu

Postaw na praktykę i zapisz się już teraz!

20-21 stycznia 2026 r.

Zaawansowane negocjacje biznesowe

17 marca 2026 r.

Standardy obsługi klienta w placówce oraz przez telefon - warsztaty dla doradców klienta

18 marca 2026 r.

Wdrażanie standardów obsługi klienta

Szkolenia mają formę stacjonarnych warsztatów opartych na praktycznych ćwiczeniach, przykładach z życia zawodowego oraz wymianie doświadczeń

Szczegółowe informacje na stronie www.bodie.pl

Zapraszamy do kontaktu:

505 459 471 | 608 522 994

511 769 808 | 505 459 553

i zgłoś swój udział: sesje@bodie.pl

ZDOBYWAJ WIEDZĘ Z NAMI!

WWW.BODIE.PL