ZWIĄZEK BANKÓW POLSKICH

DR TADEUSZ BIAŁEK

PREZES

Warszawa, 23 czerwca 2025 r.

Pan
Bartosz Drej
Zastępca Dyrektora
Departament Rozwoju Rynku Finansowego
Ministerstwo Finansów

sygn. sprawy: FN7.056.1.2025

Szanowny Panie Dyrektorze,

w odpowiedzi na pismo z dnia 17 kwietnia 2025 r. przekazuję odpowiedź Związku Banków Polskich *na prośbę o rozpatrzenie petycji w zakresie wniosku o wypracowanie dodatkowych zabezpieczeń transakcji, procedur awaryjnych, edukacji, prewencji oraz współpracy sektorowej.*

Doświadczenia sektora na gruncie bezpieczeństwa obrotu płatniczego, wskazują, że najczęstszą obecnie przyczyną utraty środków przez klientów **nie są incydenty związane z bezpieczeństwem cyfrowym infrastruktury bankowej czy infrastruktury transakcyjnej**, a działalność przestępców wyłudzających pieniądze od klientów przy zastosowaniu metod inżynierii społecznej (socjotechnik i manipulacji).

Odnosząc się do zaprezentowanych przez Fundację Dobre Państwo informacji o wykorzystywaniu instrumentu płatniczego jakim jest BLIK do wyłudzania pieniędzy, należy zauważyć, że oszustwa wykorzystujące socjotechnikę nie rozróżniają instrumentów płatniczych, a sam BLIK w ocenie ZBP nie wydaje się stanowić instrumentu o wyższym poziomie ryzyka niż pozostałe instrumenty płatnicze.

Do kradzieży w następstwie manipulacji może zostać wykorzystany przelew bankowy (w tym przelew natychmiastowy), karty płatnicze (w przypadku oszustwa, w którym użytkownik instrumentu płatniczego spodziewając się zapłaty za towar, wykorzystuje instrument płatniczy i w rzeczywistości zasila cudze konto) czy nawet gotówka przekazana w popularnym oszustwie *na policjanta*. Dlatego prosimy o nieużywanie sformułowania "przestępstwo na BLIK", bo jest ono krzywdzące i narusza dobre imię BLIK. Zauważamy, że funkcjonalności blik są rozwiązaniami nie tylko wygodnymi i innowacyjnymi ale przede wszystkim bezpiecznymi.

Zauważamy, że środowisko cyfrowe obrotu transakcyjnego jest bezpieczne. Banki powszechnie stosują dwuetapowe uwierzytelnienie. Nie brak jest również rozwiązań prawnych chroniących użytkowników instrumentów płatniczych. W świetle ustawy o usługach

ul. Kruczkowskiego 8, 00-380 Warszawa, tel.: 22 48 68 113, e-mail: aleksandra.sadowska@zbp.pl

płatniczych, dostawca usług płatniczych, który nie wymaga silnego uwierzytelnienia ponosi wobec płatnika odpowiedzialność za nieautoryzowane transakcje płatnicze dokonane z jego rachunku[1]. Podobnie, w przypadku transakcji nieautoryzowanych, banki zobligowane są do przywrócenia rachunków użytkowników do stanów jakie istniałby, gdyby nieautoryzowane transakcje nie miały miejsca w terminie maksymalnie jednego dnia od dnia otrzymania zgłoszenia o wystąpieniu nieautoryzowanej transakcji.

Od wielu lat w sektorze bankowym standardem jest przebieg transakcji opierający się na dwuskładnikowym uwierzytelnieniu, które ma zastosowanie nie tylko w tradycyjnych instrumentach płatniczych, ale także w przypadku transakcji realizowanych przy użyciu BLIK. By zlecić wypłatę, użytkownik musi nie tylko zalogować się do aplikacji mobilnej banku (1 etap uwierzytelnienia), wygenerować kod przypisany konkretnej operacji, ale także uwierzytelnić transakcję, np. odciskiem palca, co zawsze poprzedza zaprezentowanie użytkownikowi **komunikatu o szczegółach dokonywanej transakcji** – użytkownik widzi, że akceptuje wypłatę pieniędzy z bankomatu czy przelew (2 etap uwierzytelnienia).

Środowisko przestępcze jest świadome, że **systemy bezpieczeństwa transakcyjnego są skuteczne, a banki tworzą tzw. „cyfrowe twierdze"**, których nie można naruszyć. Dlatego też, od wielu lat ataki przestępców skoncentrowane są na podatnych na manipulację klientach. **Pomimo szeregu działań podejmowanych w celu minimalizowania występowania transakcji oszukańczych**, wciąż większość z sytuacji, w których dochodzi do przestępstw, pozostaje **poza kontrolą banków bo koncentrują się one na klientach – uczestnikach obrotu płatniczego.**

Ogromny problemem jest to, że zmanipulowani klienci niejednokrotnie samodzielnie dokonują na rzecz przestępców przelewów, fizycznie przekazują im środki albo udostępniają informacje potrzebne do logowań do bankowości elektronicznych, po czym umożliwiają przestępcom wyprowadzanie swoich środków z kont, uwierzytelniając transakcje, niezależnie od treści prezentowanych im komunikatów autoryzacyjnych. Przestępcza inżynieria społeczna osiągnęła tak wysoki poziom, że odnotowujemy sytuacje, w których zmanipulowani klienci przekazują przestępcom pieniądze nawet wówczas, gdy bank indywidualnie w danej sytuacji skontaktował się z nimi i ostrzegł o ryzyku utraty pieniędzy.

Powyższe obrazuje, że pomimo postępu technologicznego **wciąż najskuteczniejszą metodą walki z transakcjami oszukańczymi są działania edukacyjne.** Związek Banków Polskich, we współpracy z bankami zorganizował w 2024 roku największą w historycznej skali, szeroko promowaną w mediach kampanię edukacyjno-informacyjną „*Bądź cyberbezpieczny*" [2] . Kampania miała za zadanie edukować konsumentów o sposobach działaniach przestępców, zwiększać świadomość w zakresie cyberbezpieczeństwa i zachęcać do zachowania ostrożności. Jej celem było również podkreślenie jak ważne w zapewnieniu bezpieczeństwa są działania samego klienta. Spoty emitowane w ramach kampanii dostarczyły wskazówek w jaki sposób konsument może zapewnić sobie bezpieczeństwo finansowe. Stosowanie hasła „*Nie pomagaj się okraść. Zobacz, jak chronić swoje pieniądze*" ma zwrócić uwagę konsumentów na to jak istotna jest ich ostrożność.

Niezależnie od powyższej inicjatywy, Związek Banków Polskich podejmuje także inne, różnorodne działania edukacyjne, wykorzystując różne kanały komunikacji, takie jak kampanie reklamowe, materiały informacyjne oraz spotkania z klientami. Treści i kanały dystrybucji są dostosowane do zróżnicowanych czynników, takich jak wiek i preferencje klientów. Zarówno ZBP, jak i banki dążą do maksymalizacji skuteczności podejmowanych działań edukacyjnych.

[1] Art. 46 ust. 4a Ustawy o usługach płatniczych z dn. 19 sierpnia 2011 r.

Ponadto w odpowiedzi na rosnące cyberzagrożenia oraz formułowane oczekiwania banków FinCERT.pl - BCC ZBP przygotowuje komunikaty, których celem jest budowanie świadomości klientów w obszarze bezpieczeństwa. W 2024 r FincERT.pl BCC ZBP na stronie: https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Lista-komunikatow-i-ostrzezen-FinCERT-pl-%E2%80%93-BCC-ZBP opublikował komunikaty, które między innymi dotyczyły podejrzanych wiadomości wysyłanych za pomocą komunikatorów, osób podszywających się pod bliskich, prób wyłudzenia kodów, a także połączeń z numerów telefonów podszywających się pod banki. W 2024 roku przeprowadzono wśród banków ankietę dotyczącą planowanej kampanii edukacyjnej pt. "Bankowcy dla Cyberbezpieczeństwa 2024". Wyniki ankiety znalazły odzwierciedlenie w przygotowanej przez zespół PR wysokobudżetowej kampanii edukacyjnej, która została przeprowadzona w telewizji oraz mediach społecznościowych – link do kampanii: https://bankiwpolsce.pl/cyberbezpieczenstwo.

Ponadto, w omawianym okresie publikowano w Internecie filmy edukacyjne z udziałem celebrytów, podcasty „Real police" – seria telenoweli dokumentalnych oraz ponownie zaprojektowano przeprowadzenie Eksperymentu społecznego. Kampania spotkała się bardzo dobrym przyjęciem i była szeroko komentowana.

FinCERT.pl – BCC ZBP aktywnie angażuje się w inicjatywy edukacyjne, które mają na celu podnoszenie świadomości i rozwój kompetencji kadry w zakresie bezpieczeństwa oraz współpracę i wymianę wiedzy w sektorze finansowym.

1) Konferencje i warsztaty

Edukacja ekspercka była prowadzona przez przedstawicieli FinCERT.pl – BCC ZBP w ramach ogólnopolskich konferencji naukowych oraz warsztatów branżowych. W tej grupie wydarzeń pojawiły się takie inicjatywy jak: Europejski Kongres Finansowy w Sopocie, tematyczny blok bankowy podczas konferencji Przestępczość Teleinformatyczna XXI w. Akademii Marynarki Wojennej w Gdyni, Forum Bezpieczeństwa Banków w Warszawie, Forum Technologii Bankowych, Konferencja SafeBank – Wyzwania w obszarze bezpieczeństwa, Warsztaty Cyberbezpieczeństwa banków i policji (CBZC), XIV edycja konferencji Bankówka 2024 organizowanej w partnerstwie z pionem ekonomicznym KGP (BZPE), Stacjonarne Posiedzenie Forum AML w Warszawie.

2) Ćwiczenia z zakresu cyberbezpieczeństwa

28 maja 2024. w Gdyni odbyła się pierwsza edycja ćwiczenia CyberFIGHT Bank.01-2024. Ćwiczenie było integralną częścią ugruntowanej w społeczności osób zajmujących się bezpieczeństwem Konferencji Naukowej Akademii Marynarki Wojennej w Gdyni „Przestępczość Teleinformatyczna XXI wieku", której współorganizatorem obok Morskiego Centrum Cyberbezpieczeństwa, Allegro.pl jest także Związek Banków Polskich i FinCERT.pl – BCC ZBP.

3) Studia podyplomowe "Przeciwdziałanie Cyberprzestępczości Finansowej"

Uruchomiono kolejną edycję studiów podyplomowych dla przedstawicieli instytucji finansowych, prokuratury i policji. Studia stanowią wspólny projekt ZBP, Uniwersytetu WSB Merito w Poznaniu i Akademii Marynarki Wojennej w Gdyni. Inicjatywa została przygotowana z myślą o pracownikach organów ścigania oraz pracownikach sektora finansowego, w szczególności banków oraz niebankowych dostawców usług płatniczych zatrudnionych w komórkach anty-fraudowych i AML-owych.

Zwracamy również uwagę na trwające na poziomie unijnym prace nad *Payment Services Regulation (PSR),* które powiązane są w istotnej części z problemem spoofingu. Treść

publikacji dotycząca działalności prezydencji polskiej wskazuje na koncentrację jej prac na przeciwdziałaniu występowaniu transakcji oszukańczych.

Walka z przestępczością powinna obejmować wszystkie etapy oszustw, w tym wczesny, związany z wykorzystywaniem platform mediów społecznościowych czy infrastruktury telekomunikacyjnej do manipulowania poszkodowanymi.

Związek Banków Polskich dostrzega również inne możliwości wykorzystania technologii w celu zapewnienia wyższego poziomu bezpieczeństwa klientów. Banki wykorzystują do walki z oszustwami zaawansowane technologie; pośród nich jest obiecująca metoda analizy behawioralnej polegająca na tworzeniu indywidualnych profili klientów korzystających z systemów bankowych na podstawie obserwowania sposobów w jaki klienci je użytkują.

W ramach analizy behawioralnej systemy bankowe analizują zmienne - takie jak pory logowań, częstotliwość uderzeń w klawiaturę, czas spędzany w danej zakładce bankowości internetowej, kwoty przelewów, ich odbiorców, etc. W oparciu o zgromadzone informacje, tworzony jest behawioralny profil klienta, a bank ma możliwość identyfikacji odchyleń, świadczących o tym, że potencjalnie to nie klient jest osobą logującą się do systemu bankowości elektronicznej lub zidentyfikować przypadek, w którym to klient jest osobą logującą się, ale jego zachowanie w takim stopniu odbiega od normalnego sposobu korzystania z aplikacji, że należy interweniować i zapobiec transakcji oszukańczej w trakcie jej dokonywania przez oszusta za pomocą socjotechniki.

Należy jednak podkreślić, że w obecnym stanie prawnym banki nie mogą wykorzystywać pełnego potencjału dostępnej technologii w walce z oszustwami - obowiązujące przepisy prawa i stanowiska organów uniemożliwiają korzystanie z technologii opartej o analizę behawioralną w każdym przypadku. Urząd Ochrony Danych Osobowych zaklasyfikował dane behawioralne jako dane szczególnych kategorii w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, w myśl czego bank może przetwarzać dane behawioralne wyłącznie w oparciu o zgodę klienta.

W praktyce oznacza to, że Bank może **korzystać z analizy behawioralnej jedynie w przypadku, w którym klient wyrazi zgodę na wykorzystanie danych behawioralnych**. Niestety, pomimo inicjatyw podejmowanych w bankach w celu zbierania tego rodzaju zgód, zgody są udzielane przez niewielu, najbardziej świadomych zagrożeń klientów. Manipulujący klientami przestępcy są również świadomi zagrożenia jakim dla ich przestępczej działalności jest analiza behawioralna, więc ich pierwszym krokiem jest doprowadzenie do wycofania zgody na wykorzystanie tej funkcji. Jesteśmy przekonani, że **analiza behawioralna osiągnęłyby pełny potencjał w momencie, w którym banki mogłyby wykorzystywać opisywane rozwiązania w szerszym zakresie, co stałoby się możliwe, w momencie zmiany otoczenia regulacyjnego.**

Ponadto, istotnym wzmocnieniem zdolności sektora finansowego do ochrony jego klientów przed ryzykiem utraty środków finansowych na skutek oszustw byłoby rozszerzenie możliwości dzielenia się informacjami stanowiącymi tajemnicę bankową z przedsiębiorcami komunikacji elektronicznej. Doświadczenia jednostek przeciwdziałających oszustwom bankowym wskazują, że incydenty bezpieczeństwa mogą mieć międzysektorowe skutki oddziaływania na usługi świadczone przez sektor komunikacji elektronicznej oraz sektor finansowy. Dlatego, dla wskazanych podmiotów krytyczne jest stworzenie możliwości szybkiego otrzymania informacji o zdarzeniach, które mogą mieć wpływ na świadczone przez nich usługi. Niestety, obecny kształt przepisów dotyczących możliwości ujawniania tajemnicy

bankowej (art. 106d ust. 1 ustawy z 29 sierpnia 1997 r. – Prawo bankowe) uniemożliwia wymianę informacji chronionej tajemnicą bankową z firmami telekomunikacyjnymi.

***

Mając na uwadze to, że transfer legalnych środków klientów banków do środowiska przestępczego nie tylko stanowi osobistą tragedię wielu osób, ale także umacnia środowisko przestępcze czyniąc je jeszcze bardziej niebezpiecznym, zapewniam, **że wspólnym priorytetem sektora bankowego jest udaremnianie transferu środków jeszcze przed wystąpieniem transakcji oszukańczych i banki podejmują wiele działań, żeby chronić użytkowników**. Należy jednak z podkreślić, że wiele działań klientów pozostaje poza kontrolą banków, a przeniesienie na sektor bankowy odpowiedzialności finansowej za każdą transakcję, zrealizowaną przez użytkowników instrumentów płatniczych niezgodnie z ich intencją jest postulatem nie do przyjęcia.

Rolą Banków jest zapewnienie stabilnej, bezpiecznej infrastruktury transakcyjnej i prawidłowe wykonywanie zleconych transakcji. Z kolei rolą organów ścigania i sądów jest ściganie przestępców, separowanie ich od społeczeństwa i wymierzanie sprawiedliwości oszukanym obywatelom.

Warto zauważyć, że polski sektor bankowy dostrzega problem transakcji oszukańczych i zjednoczył swoje działania, pomimo konkurowania w innych obszarach, od wielu lat współpracuje ze sobą na rzecz bezpieczeństwa obrotu płatniczego, angażując znaczne środki na cyberbezpieczeństwo, trwale doskonaląc narzędzia zapewniające bezpieczeństwo i edukując klientów, czego dowód stanowi załączony do niniejszego pisma wykaz inicjatyw podejmowanych przy Związku Banków Polskich przez sektor.

Podkreślam jednocześnie, że walka ze środowiskiem przestępczym wymaga zaangażowania najlepszych możliwych technologii. Dlatego też deklaruję pełną gotowość sektora bankowego do aktywnego udziału we wszelkich inicjatywach legislacyjnych, które będą miały na celu poprawę bezpieczeństwa klientów, podkreślając znaczenie w poprawie bezpieczeństwa, wspomnianej w niniejszym piśmie analizie behawioralnej.

Z poważaniem,

Signed by /
Podpisano przez:

Tadeusz Białek

Date / Data:
2025-06-23
14:54

ul. Kruczkowskiego 8, 00-380 Warszawa, tel.: 22 48 68 113, e-mail: aleksandra.sadowska@zbp.pl