„Razem możemy więcej" – również w obszarze cyberbezpieczeństwa

Rozmowę z **Rafałem Bednarkiem**, wiceprezesem zarządu Biura Informacji Kredytowej na temat bezpieczeństwa w sieci przeprowadziła **Aleksandra Rączkiewicz**.

Defraudacje i wyłudzenia kredytów wciąż pozostają jednym z najważniejszych wyzwań, z którymi mierzy się sektor finansowy. Banki i instytucje finansowe stosują różne metody wykrywania działań przestępczych. W jaki sposób BIK może wesprzeć banki spółdzielcze w tych działaniach?

Fraudy, a w szczególności fraudy kredytowe, są cały czas dużym wyzwaniem w sektorze finansowym. Corocznie robimy w BIK analizę, której celem jest określenie skali tego zjawiska w polskich bankach. Analizujemy, jaki jest wolumen i wartość kredytów, w przypadku których istnieje uzasadnione podejrzenie, iż są to zobowiązania zaciągane bez intencji spłaty. Dla przykładu myślę tutaj o takich kredytach, w przypadku których klient nie zapłacił nawet jednej raty po ich zaciągnięciu lub trwale przestał regulować swoje zobowiązania wobec banku po zapłacie jednej lub dwóch rat. Oczywiście mogą tu pojawić się jakieś przypadki losowe, jednak to raczej wyjątki od reguły. W zdecydowanej większości za takimi przypadkami kryje się brak intencji zwrotu pożyczonych środków od samego początku. Kiedy mamy do czynienia z kredytem zaciąganym bez intencji spłaty możemy mówić o fraudzie. To tak, jakby ktoś poszedł do restauracji, zamówił obiad i od początku nie miał zamiaru za niego zapłacić. Wyniki tych analiz wskazują, że tylko w portfelu kredytów dla osób fizycznych w bankach, takich przypadków jest rocznie na ok. 600 mln zł. Doświadczenia minionych kryzysów i okresów spowolnienia wskazują ponadto, że w takich czasach jak obecnie ryzyko wyłudzeń jeszcze wzrasta. Fraudy nie omijają też banków spółdzielczych, które tracą kilkadziesiąt mln zł rocznie z tego powodu. To ogromna kwota.

Mając na względzie skalę wyzwania oraz znając antyfraudowe rozwiązania sektorowe na innych zaawansowanych rynkach, postanowiliśmy kilka lat temu zbudować w BIK Platformę Antyfraudową, której fundamentem jest ścisła współpraca banków i innych pożyczkodawców w zwalczaniu fraudów kredytowych. Podobnie jak tradycyjnie wymiana informacji o poziomie zadłużenia klienta i jego historii kredytowej poprzez BIK pomaga ograniczać bankom koszty ryzyka kredytowego, tak Platforma Antyfraudowa BIK i wymiana danych o klientach dokonujących fraudów pomaga kredytodawcom skutecznie bronić się przed atakami z ich strony i stratami z powodu wyłudzeń. Cały mechanizm wbudowany w Platformę jest oczywiście bardzo złożony i opiera się na licznych regułach, danych, zaawansowanej analityce i rozpoznawanych ciągle nowych schematach wyłudzeń, jednak ogólne przesłanie jest podobne do tego, które często słyszę wśród banków spółdzielczych – „Razem możemy więcej". Fundament to szeroka współpraca w zakresie przeciwdziałania wyłudzeniom kredytowym, w której banki wzajemnie się ostrzegają via BIK o potencjalnych działaniach przestępców. Rozwiązanie to funkcjonuje na rynku od listopada 2017 r. Platforma Antyfraudowa BIK potwierdziła już swoją skuteczność. Pomimo, że mówimy o początkowym okresie jej funkcjonowania, gdzie stopniowo dołączały kolejne banki (obecnie uczestniczy w niej 8 podmiotów i kilkanaście kolejnych realizuje projekty podłączeniowe), od momentu jej uruchomienia w listopadzie 2017 r. do końca maja br. sektor bankowy uniknął już dzięki niej wyłudzeń o wartości 244 mln zł.

Banki spółdzielcze także potwierdzają zainteresowanie Platformą Antyfraudową. Przykładem może być zainicjowany przez grupę banków spółdzielczych projekt wdrożenia Platformy Antyfraudowej, nie w pojedynkę, lecz we współpracy, w celu wyeliminowania strat wynikających z wyłudzeń. Ta inicjatywa realizowana jest obecnie we współpracy z Centrum Rozwoju Usług Zrzeszeniowych (CRUZ), które świadczyć będzie różnego rodzaju usługi, w tym usługę analizy antyfraudowej na rzecz banków spółdzielczych. Alert antyfraudowy wysyłany do banku w związku z uzasadnionym podejrzeniem wyłudzenia wymaga bowiem pogłębionej analizy. W ramach tej inicjatywy banki postanowiły, że takie pogłębione badanie może być realizowane na ich rzecz w CRUZ. Prowadzimy też oczywiście rozmowy na ten temat z Bankiem SGB. Tutaj podobnie chodzi o implementację Platformy Antyfraudowej dla większej liczby banków, a docelowo dla całego Zrzeszenia.

Jakie elementy wyróżniają Platformę Antyfraudową BIK na tle innych, dostępnych na rynku, rozwiązań?

Platformę Antyfraudową BIK charakteryzuje innowacyjne podejście, rozumiane jako współdzielenie informacji o nadużyciach pomiędzy wszystkimi uczestnikami wspólnego systemu, co – jak wcześniej wspomniałem – ma istotne znaczenie dla skutecznej ochrony przed nadużyciami. System ma charakter prewencyjny. To m.in. dzięki wzajemnemu ostrzeganiu się jego uczestników o podejrzanych przypadkach, niosących ze sobą ryzyko nadużycia, efektywność wykrycia istotnie wzrasta. Wartością jest współpraca – to klucz do sukcesu w walce z ograniczeniem strat zarówno po stronie klienta, jak i banku. Można nawet powiedzieć, że rozwiązanie to wyłoniło się ze współpracy. Geneza jest bowiem taka, iż w ramach wspólnej dyskusji przedstawicieli banków i BIK na kolejnych warsztatach wypracowaliśmy model, który odwoływał się do najlepszych praktyk światowych, ale też wpisywał się w polskie uwarunkowania prawne potwierdzone praktyką i doświadczeniami banków.

Gdy mówimy o Platformie, trudno nie wymienić nowoczesnych technologii, dzięki którym możliwe jest działanie tego rozwiązania, tj. procesu ostrzegania o fraudach w czasie rzeczywistym. Tylko w taki sposób można zapewnić skuteczną ochronę przed dynamicznie działającymi przestępcami i szybko modyfikowanymi schematami oszustw. Gwarantuje to ponad 150 reguł i algorytmów systemu, które weryfikują wnioski kredytowe i wyszukują podejrzane powiązania i przejawy nadużyć. Zarówno raporty, jak i alerty antyfraudowe są natychmiast, w trybie online, wysyłane uczestnikom Platformy Antyfraudowej BIK.

Podstawą technologiczną Platformy jest system „Hunter II" opracowany przez partnerską firmę Experian. Również wykorzystując inny system tego dostawcy „Fraudnet" – BIK stworzył dedykowane na rynek polski rozwiązanie służące ochronie kanałów online – Platformę Cyber Fraud Detection (CFD). Rozwiązania te sprawdziły się na innych zaawansowanych rynkach m.in. w Wielkiej Brytanii, Włoszech, Francji, Hiszpanii, RPA czy Stanach Zjednoczonych. Systemy te są w pełni zintegrowane z systemami BIK i dostosowane do naszego kontekstu prawnego. Za wspomnianym partnerstwem nie stoi oczywiście tylko technologia, ale również głęboka wiedza biznesowa w obszarze antyfraudowym, zbudowana na różnych rynkach.

Muszę tu koniecznie wspomnieć też o wyjątkowej ekspertyzie antyfraudowej, którą udało nam się zbudować w BIK. Stworzyliśmy liczny zespół osób, które mają gruntowne doświadczenie w pracy w komórkach antyfraudowych najbardziej zaawansowanych pod tym względem banków i firm technologicznych. Ekspertyza ta została uzupełniona doświadczeniem współpracy z naszym partnerem technologicznym i z każdym kolejnym klientem. BIK prowadzi stałe konsultacje ze swoimi klientami. Proponując przystąpienie do Platformy Antyfraudowej BIK, oferujemy bankom doradztwo biznesowe i transfer wiedzy. Staramy się dzielić naszym doświadczeniem pokazując, jak można optymalizować działania prewencyjne, wzmacniać ochronę sektorową i sprawnie ostrzegać się o podejrzanych przypadkach, niosących ze sobą ryzyko nadużycia.

Na koniec jeszcze raz chciałbym powiedzieć o skuteczności rozwiązania. Wspominałem o ponad 240 mln potencjalnych fraudów, które zostały zatrzymane w sektorze bankowym. Poszczególne banki chwalą się często, że ich zwrot z inwestycji następuje w pojedynczych miesiącach. To chyba najsilniejszy argument.

Czy w ostatnim czasie zauważyli Państwo większe niż dotychczas zainteresowanie wdrożeniem przez banki Platformy Antyfraudowej?

Porównując dwa miesiące przedpandemiczne (styczeń i luty 2020 r.) do okresu pandemicznego, trwającego od marca br., zaobserwowano 35-procentowy wzrost liczby wniosków, które Platforma Antyfraudowa BIK wskazała do weryfikacji jako ewentualne próby nadużyć. Istotne jest to, że wystąpiło to przy jednoczesnym spadku aktywności kredytowej w sektorze bankowym.

Mamy także potwierdzenie, że w czasie kryzysu COVID-19 instytucje finansowe stają się bardziej ostrożne i częściej odpytują system PAF. Liczba zapytań o Bankowy Raport Antyfraudowy (BRA), kierowana do PAF ze strony banków w okresie pandemii wzrosła o 7%.

Obserwacje te są zatem ewidentnym potwierdzeniem, że w okresie kryzysu – pandemii rozwiązanie systemowe, sektorowe stało się jeszcze bardziej potrzebne do przeciwdziałania stratom z tytułu wyłudzeń. Pracujemy też z kolejnymi bankami nad dołączeniem do Platformy. W wielu bankach projekty przyłączeniowe zyskały wyższy priorytet w kontekście możliwej recesji.

Niezwykle ważnym działaniem w kontekście cyberbezpieczeństwa jest prowadzenie przez banki działań o charakterze edukacyjnym. W jaki jeszcze sposób bank spółdzielczy może chronić swoich klientów w celu minimalizacji ryzyka wyłudzeń?

Bezpieczeństwo należy traktować jako współodpowiedzialność. Działania firm i ich klientów powinny iść w parze, aby minimalizować zagrożenia ze strony cyberprzestępców. Faktycznie bardzo ważna jest edukacja. Żaden system nie zabezpieczy ostatecznie klientów, jeśli oni sami wykażą się niefrasobliwością lub niewiedzą w zakresie podstawowych zasad bezpieczeństwa. Przestępcy cały czas stosują socjotechniki i nowe, niekiedy wymyślne sposoby uzyskania dostępów do credentiali klientów. W ostatnim okresie obserwujemy nasilające się ataki, gdzie wątkiem przewodnim jest ochrona zdrowia w okresie pandemii, ochrona oszczędności w okresie turbulencji czy możliwość skorzystania z kolejnych działań pomocowych. Działania uświadamiające i komunikacja z klientami jest w tym kontekście niezmiernie ważna.

Kluczowa jest jednak również skuteczność mechanizmów zabezpieczających w bankach. Dużo rozmawiamy tu o systemach antyfraudowych. Jeśli np. taki system w banku skutecznie wykryje oszusta, który używając skradzionej tożsamości próbuje wyłudzić kredyt, to oczywiście bank chroni się przed stratą ale chroni też osobę, której tożsamość została nieuczciwie użyta. Kolejny, wydaje się oczywisty przykład, to skuteczne zabezpieczenie bankowości elektronicznej. Mechanizm rozpoznawania skompromitowanego urządzenia, z którego następuje próba logowania do konta klienta – funkcjonalność taką posiada dla przykładu wspomniany wcześniej, oferowany przez BIK system Cyber Fraud Detection (CFD) – jest istotną ochroną klientów banku. Mechanizmy te są tym skuteczniejsze, na ile wiążą się ze współdziałaniem całego sektora. A takie właśnie podejście w obszarze antyfraudowym i cyberbezpieczeństwa proponujemy w BIK.

Jednym z rozwiązań oferowanych klientom banków przez BIK są Alerty – na czym polegają? Czy kiedy rozpoczęła się pandemia COVID-19 zaobserwowali Państwo wzrost korzystania przez klientów indywidualnych z Alertów BIK?

Fundament to szeroka współpraca w zakresie przeciwdziałania wyłudzeniom kredytowym, w której banki wzajemnie się ostrzegają via BIK o potencjalnych działaniach przestępców.

Alerty BIK to kompleksowe ostrzeżenie osoby przed wyłudzeniami „na nasze dane". Co ważne, jest to usługa automatyczna – sama pilnuje, czy ktoś nie posłużył się naszymi danymi. Można je aktywować bez wychodzenia z domu, na stronie internetowej www.bik.pl. Potwierdzenie tożsamości odbywa się z wykorzystaniem danych z dowodu osobistego oraz przelewu weryfikacyjnego, a cały proces nie trwa dłużej niż kilka minut. Po potwierdzeniu tożsamości użytkownika, usługa zaczyna działać niemal natychmiast i jest aktywna 24 godziny, 7 dni w tygodniu, przez 12 miesięcy.

Alerty BIK przesyłane są za pomocą maila i SMS-a, za każdym razem, gdy w BIK pojawi się zapytanie o historię kredytową, będące częścią procesu kredytowego. Powiadomienia także przyjdą każdorazowo, gdy ktoś próbuje np. podpisać umowę leasingową czy zawrzeć umowę z dostawcą energii albo gazu.

W praktyce działa to tak, że jeśli klient sam nie składał żadnych wniosków o kredyt, nie kupował nic na raty, nie poręczał kredytu itp., to pojawienie się Alertu może oznaczać, że ktoś próbuje wziąć kredyt na jego skradzione dane. Dzięki informacji z Alertu i podjęciu właściwych działań klient ma szansę szybko i skutecznie zareagować na niepokojące sygnały.

W Alercie podana jest data zdarzenia, nazwa instytucji, w której złożono wniosek na dane klienta oraz numer infolinii BIK – na wypadek, gdyby potrzebne było wsparcie w wyjaśnieniu sprawy. W przypadku stwierdzenia próby wyłudzenia, BIK natychmiast przekazuje do instytucji finansowej informację o zablokowaniu zapytania i zobowiązania. Nasi konsultanci pomagają także w kontaktach klienta z policją czy prokuraturą.

Myślę, że wzmożona aktywność internetowa w okresie pandemii może skłaniać do korzystania z takich narzędzi wspomagających. Oczywiście należy także zachowywać inne środki ostrożności. Przeprowadzone na nasze zlecenie w marcu i ponownie w kwietniu br. badania opinii potwierdziły wręcz, że Polacy boją się zarówno o swoje zdrowie, jak i finanse. Zdaniem 40% badanych zawirowania związane z koronawirusem mogą spowodować zmniejszenie bezpieczeństwa transakcji płatniczych w sieci. A tych w ostatnim czasie przybywa, szczególnie w związku z częstszymi zakupami internetowymi.

Pozytywne jest to, że ponad połowa Polaków zadeklarowała, że zamierza podjąć działania zwiększające bezpieczeństwo haseł dostępu do kont bankowych czy poczty mailowej. Postanowiliśmy to zweryfikować, zlecając ponowne badanie w kwietniu. Jak się okazało, deklaracje nie idą w parze z prewencją. Choć Polaków cechuje świadomość zagrożeń, to aż ponad połowa osób (51%) przyznała, że nie zna żadnych, powszechnie dostępnych usług ochronnych i nigdy z nich nie korzystała. Co gorsza, 28% nigdy ich nie miała, wręcz nie interesowała się nimi i nie planuje skorzystać.

Polacy nadal więc nie podejmują wystarczających działań, by zwiększyć swoje bezpieczeństwo i ustrzec się przed konsekwencjami kradzieży tożsamości, w tym dotkliwą stratą materialną.

Należy w tym miejscu podkreślić, że Alerty BIK to jedyna usługa w kraju, obejmująca tak szeroką ochroną zakres wyłudzeń. Ma największe pokrycie rynku ze względu na to, że BIK współpracuje ze wszystkimi bankami komercyjnymi, bankami spółdzielczymi, SKOK-ami oraz prawie wszystkimi firmami pożyczkowymi w Polsce (w tym największymi i wszystkimi firmami pożyczkowymi, działającymi on-line). Ponadto zakres informacji wykorzystywanych w Alertach BIK zwiera również informacje, pochodzące z Rejestru Dłużników BIG InfoMonitor – swojej spółki córki, a więc dane z firm telekomunikacyjnych, spółek energetycznych, jednostek samorządu terytorialnego, firm leasingowych i faktoringowych.

Chętnie też, jako BIK, włączamy się w akcję „Czerwiec z bankiem spółdzielczym". Kibicujemy inicjatywom kierowanym do banków spółdzielczych oraz ich klientów. Potrzebna jest bowiem nieustanna edukacja, wskazująca na dostępność narzędzi i usług antyfraudowych, możliwych do samodzielnego aktywowania przez każdego z osobna, indywidualnie.