

Biometria Behawioralna w cyberbezpieczeństwie



BIG
InfoMonitor



DFP
Digital Fingerprints

GRUPA BIK



Michał Łukasiewicz

Lider Strumienia Antyfraudowego, Biuro Informacji Kredytowej
Członek Zarządu Digital Fingerprints

Problem phishing, smishing, vishing...

Kradzież haseł jest coraz większym zagrożeniem, w ten sposób kradnie się ponad 3 miliardy dolarów rocznie

Kradzież sesji jest wciąż możliwa mimo starań całego sektora bezpieczeństwa

Nie ma idealnej metody na wykrycie przejęcia konta

Walka z fraudami jest syzyfową pracą nawet dla najlepiej przygotowanych organizacji



Phishing

Grupy przestępcze coraz częściej i coraz zuchwalej podszywają się pod autentyczne serwisy transakcyjne banków. Najbardziej zaawansowane phishing kity wyłudniają też jednorazowy kod SMS, i automatycznie dodają rachunek zaufany do konta ofiary.



Friendly Frauds

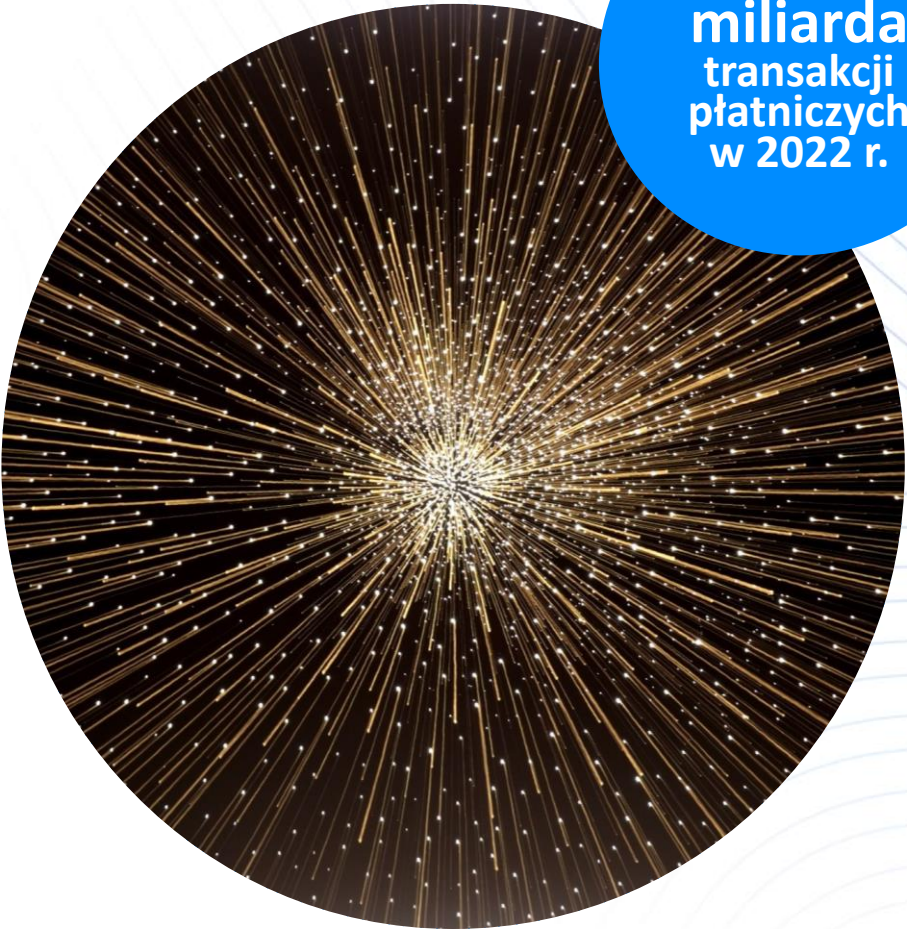
Zgodnie z wymogami PSD2, banki są zobowiązane do zwrotu środków płatnikowi w ciągu 1 dnia roboczego jeżeli doszło do nieautoryzowanej transakcji. Może prowadzić to do sytuacji gdzie właściciele kont zaczną pozorować nieautoryzowane transakcje w celu wyłudzenia odszkodowania.



False investments

Za pomocą serwisów społecznościowych przestępcy namawiają ofiary do zainstalowania klienta zdalnego pulpitu celem dokonania inwestycji. Następnie przestępca wyprowadza środki z konta ofiary, często dodatkowo zaciąga w jej imieniu kredyty.

Skala wyzwania



**3,7
miliarda**
transakcji
płatniczych
w 2022 r.



42 miliony
umów
bankowości
elektronicznej



22 miliony
aktywnych
użytkowników

Transakcje oszukańcze w 2022

Wyłudzenia dokonane w wyniku kradzieży danych osobowych obawia się dwie trzecie dorosłych Polaków (65%), w tym 23% ma zdecydowane obawy - częściej wyrażają je kobiety (26%) niż mężczyźni (20%). Obaw o wyłudzenie nie odczuwa co piąty Polak (22%).

Co najmniej jednego zagrożenia wyłudzeniem doświadczyło osobiście 36% Polaków.

KOSZT

11,5

mln zł wartość strat poniesionych przez banki (polecenie przelewu)

RYZIKO

198

mln zł wartość operacji oszukańczych

MOBILE

47%

ilościowo

TREND

2x

Roczna ilość transakcji oszukańczych podwajała się od 2020 roku

SKALA

54k

Ponad 54 tysiące transakcji oszukańczych (polecenie przelewu)

WEB

74%

wartościowo

Digital Fingerprints



GRUPA BIK



DFP

Digital Fingerprints

- Digital Fingerprints to firma z branży cyberbezpieczeństwa specjalizująca się w biometrii behawioralnej. Prace badawcze zostały uruchomione w 2017 r. w ramach funduszu mAccelerator, a **od 30 maja 2022 r. Digital Fingerprints jest częścią Grupy Biura Informacji Kredytowej.**
- Rozwiązanie dostarczane przez Digital Fingerprints **weryfikuje tożsamość** użytkowników systemu poprzez analizę interakcji użytkownika z **urządzeniem.**
- Wdrożenia produkcyjne w 2 bankach w Polsce.
- Ponad 2 mln klientów objętych ciągłą ochroną.
- Co dalej ? budowa sektorowego systemu biometrii behawioralnej w oparciu o rozwiązanie spółki Digital Fingerprints, oraz kompetencje Grupy BIK.



Rozwiązanie – biometria behawioralna



GRUPA BIK



Niezauważalnie zbieramy zachowanie użytkownika

wspieramy aplikacje przeglądarkowe (klawiatura i mysz) i aplikacje mobilne (dedykowane SDK)



Nauczmy się jego zachowań

Niech każdy użytkownik ma więcej niż jeden osobisty model, który cały czas się dostosowuje do jego nawyków



Reagujemy w czasie rzeczywistym

Zapobiegamy stratom zanim do nich dojdzie



Zbieramy zanonimizowane zachowanie klienta przy pomocy skryptu-agenta w serwisie transakcyjnym Banku



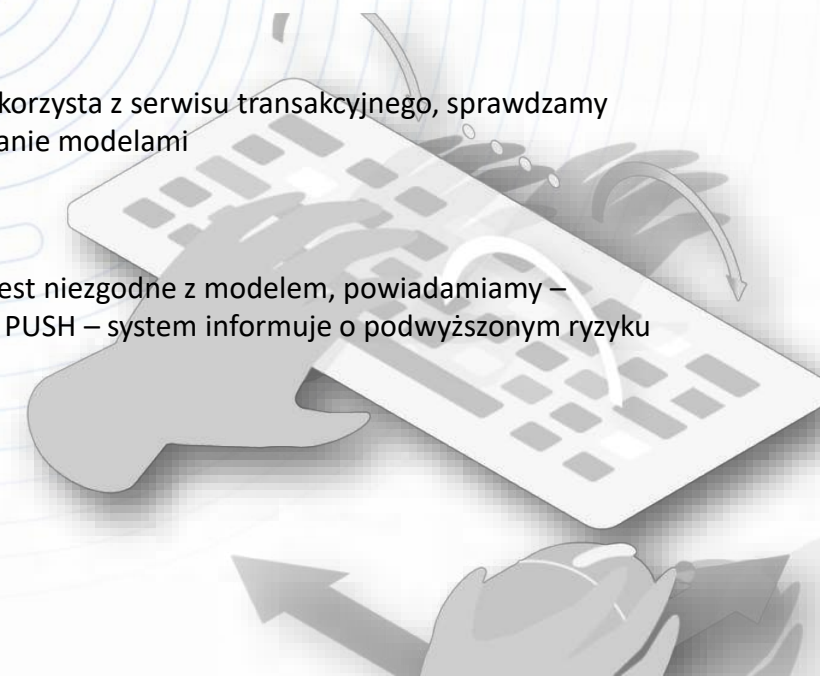
Zebrane wartości przekształcamy matematycznie do ponad 80 cech, które np. opisują sposób w jaki Klient pisze na klawiaturze



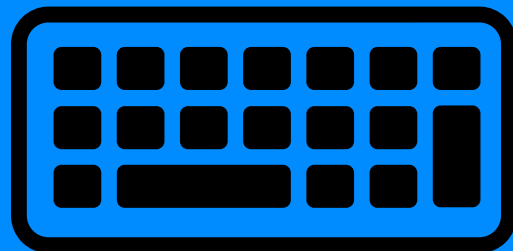
Podczas gdy klient korzysta z serwisu transakcyjnego, sprawdzamy każde jego zachowanie modelami



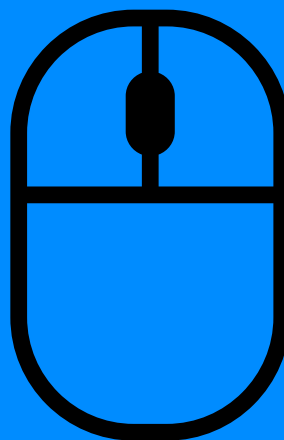
Jeżeli zachowanie jest niezgodne z modelem, powiadamiamy – komunikatem typu PUSH – system informuje o podwyższonym ryzyku



Inżynieria cech – jakimi danymi dysponujemy?



CZAS WCIŚNIĘCIA
CZAS PUSZCZENIA
GRUPA KŁAWISZOWA



CZAS KLIKNIĘCIA
WSPÓŁRZĘDNE KURSORA
UŻYCIE SCROLLA

SESJA PRZEGLĄDARKOWA

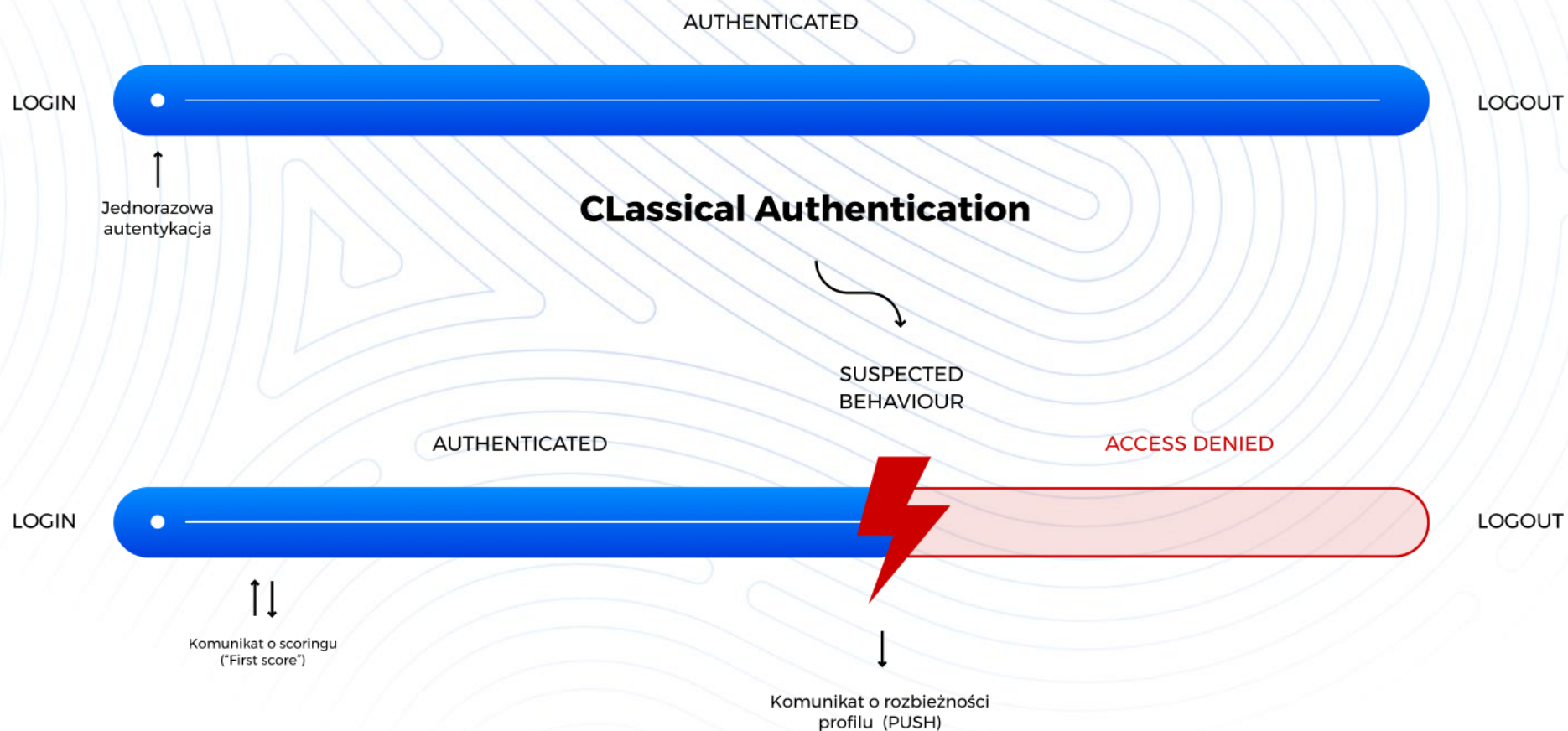


ODCZYTY Z SENSORÓW
KŁAWIATURA EKRANOWA
KONTAKT Z EKRANEM

APLIKACJA MOBILNA

Autentykacja ciągła

Ciągła autentykacja chroni od momentu **zalogowania** się aż do **końca** sesji.
Dzięki temu możemy zareagować zanim dojdzie do utraty środków.



Zastosowanie biometrii

- **Weryfikacja tożsamości użytkownika** - niewidzialny czynnik autoryzacyjny, który nie wymaga od użytkownika nauki
- **Wykrywanie ataków** – nawet tych, które uważa się za niewykrywalne konwencjonalnymi narzędziami, takie jak vishing, man in the browser, dostęp przez różne warianty zdalnego zarządzania komputerem czy klonowanie kart SIM



Przykład 1:

Po przejęciu loginu i hasła do konta, przestępca załogował się na konto ofiary. Przy próbie logowania się przestępcy, system wykrywa inne zachowanie.



Przykład 2:

Klient zostaje naciągnięty na fałszywą inwestycję przy pomocy zdalnego pulpitu. Gdy przestępca wpisuje dane do przelewu, system alertuje Bank.



Przykład 3:

System regulowy wykrywa podejrzaną transakcję. Biometria behawioralna potwierdza, że transakcja została wprowadzona przez właściciela konta, pozwalając na wyciszenie false positive.

Strong Customer Authentication



Regulacja Payment Services Directive 2 (PSD2) nakłada na banki wymóg silnej weryfikacji tożsamości klienta.

Biometria Behawioralna jest uznana za metodę silnej autoryzacji klienta przez European Banking Authority. Banki korzystające z Biometrii Behawioralnej nie muszą implementować innych mechanizmów autoryzacji, takich jak tokeny SMS, albo aplikacje mobilne.

Rozwiązanie dostarczane wspólnie przez Digital Fingerprints i BIK może być traktowane jako unikalną cechę użytkownika (Inherence) stanowiący jeden z elementów SCA.

O konieczności stosowania SCA wypowiada się również KNF.

WIEDZA



Coś, co wie tylko użytkownik
(np. hasło)

POSIADANIE



Coś, co posiada wyłącznie użytkownik
(np. telefon, token, karta)

CECHA UŻYTKOWNIKA



Coś, co jest cechą charakterystyczną użytkownika
(np. odciska palca, biometria behawioralna)

Jakość rozwiązania - KPI

- Modele budowane są pod kątem rozróżniania danego użytkownika od innych
- Jakość modeli szacowana jest na podstawie rozróżniania użytkownika od innych (1) i zdolności detekcji oszustów (2)

1. Poprawność rozpoznania klientów przy logowaniu

Kanał WEB

96%

rozpoznanie
klienta

Kanały mobile

95%

rozpoznanie
klienta

2. Wykrycie nieautoryzowanego dostępu podczas logowania

90%

rozpoznanie
fraudu

90%

rozpoznanie
fraudu

Krok dalej - rozwiązanie sektorowe (1)



GRUPA BIK

✓ WSPÓŁTWORZENIE MODELII	Modele tworzą się na podstawie danych z wszystkich banków z których korzysta użytkownik.
✓ BUDOWANE INDYWIDUALNIE DLA KAŻDEGO UŻYTKOWNIKA	Każdy chroniony użytkownik ma dedykowany dla niego zestaw modeli behawioralnych.
✓ DANE BEZKONTEKSTOWE	Potrzebujemy wiedzieć tylko jak użytkownik pisze, a nie co pisze.
✓ WSPÓŁDZIELENIE MODELII	Klient nowy lub rzadko logujący się do swojego konta może posiadać swój profil zbudowany w innym banku, dzięki temu jest cały czas chroniony.
✓ WSPÓLNA BAZA DANYCH POWODUJĄCA OBNIŻENIE KOSZTÓW	Im więcej użytkowników w rozwiązaniu sektorowym tym ochrona jest tańsza – osiągamy efekt synergii na poziomie funkcjonalnym i kosztowym.

Krok dalej - rozwiązanie sektorowe (2)

- Klient jest w centrum rozwiązania sektorowego
- Cechy biometryczne mierzone w spójny sposób
- Wspólne profile behawioralne
- Szybkie budowanie profili biometrycznych
- Natychmiastowe wdrożenie ochrony dla nowego klienta



Q&A



GRUPA BIK



Michał Łukasiewicz

Członek Zarządu Digital Fingerprints,
Lider Strumienia Antyfraudowego w BIK S.A.

michal.lukasiewicz@fingerprints.digital

Wykrywanie vishingu
i phishingu

Identyfikacja
“friendly frauds”

Optymalizacja
monitorowania
transakcji

