

Biometria behawioralna zaporą dla cyberprzestępców

„Melodia pisania” na klawiaturze laptopa, komputera czy smartfonu pokrzyżuje plany cyberprzestępców. To nie science fiction, to rzeczywistość.



FOT. BIK SA

Dr Mariusz Cholewa

PREZES ZARZĄDU
BIURO INFORMACJI KREDYTOWEJ SA

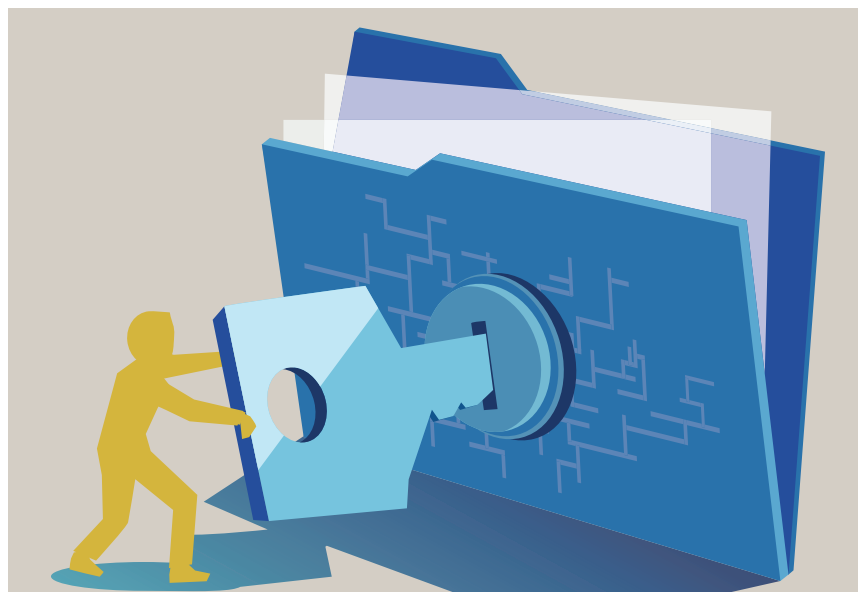
Biurowo Informacji Kredytowej inwestuje w spółkę Digital Fingerprints i wdraża rozwiązanie antyfraudowe, jakiego jeszcze nie było w sektorze finansowym w Polsce.

To innowacyjna technologia, która z pomocą algorytmów matematycznych i sztucznej inteligencji, tworzy unikalne profile zachowań użytkowników, służące identyfikacji konkretnej osoby w momencie logowania się jej do konta – czy to z komputera, czy z urządzenia mobilnego. **Jeśli ktoś niepowołany posługuje się czyimiś danymi do logowania do banku, system wykryje oszusta w czasie rzeczywistym, niezależnie od aplikacji czy urządzenia, z jakiego korzysta.**

JESTEŚMY NIEUSTANNIE NA CELOWNIKU CYBERPRZESTĘPCÓW

Włamanie na konta bankowe w wyniku kradzieży haseł, podszywanie się pod serwisy transakcyjne banków, instalowanie zdalnych pulpitów celem dokonania inwestycji z konta ofiary – to tylko niektóre spośród działań cyberprzestępczych z wykorzystaniem skradzionych danych osobowych i chwytów socjotechnicznych w celu wyludzeń kredytów i pieniędzy.

Pozytywne aspekty cyfryzacji praktycznie wszystkim użytkownikom sieci zakłóca cyberprzestępczość zagrażająca bezpieczeństwu osobistych danych.



FOT. FEODORA/STOCK.ADOBE.COM

Większość z nas, bo aż 95%, na co dzień korzysta z internetu. Co więcej, w siłę rośnie bankowość internetowa, z której korzysta 21 mln osób. Dogania ją grupa aktywnych użytkowników bankowych aplikacji mobilnych, na koniec czwartego kwartału 2021 r. korzystało z niej ponad 16,5 mln użytkowników.

To poważna część naszego społeczeństwa, która ma przy tym świadomość niebezpieczeństwa, jakim jest kradzież ich danych. Wyludzenia kredytów na skradzione dane boi się 54% Polaków, a aż 84% obawia się wykorzystania swoich personaliów w wyniku wycieku. I nie ma w tym nic dziwnego, bo chodzi przecież o bezpieczeństwo pieniędzy, często oszczędności naszego życia.

Niepokoje ponadto coraz częściej odnotowywany zorganizowany charakter nielegalnej działalności w przestrzeni online, często z wykorzystaniem technologii IT. Ataki hackerskie stanowią zagrożenie zarówno dla instytucji, jak i osób prywatnych.

Wyzwaniem staje się zatem przeciwdziałanie tym przestępstwom – i to w sposób systemowy i zintegrowany, łączący instytucję, urządzenie mobilne i konsumenta. W Biurze Informacji Kredytowej znaleźliśmy na to sposób, inwestując w spółkę Digital Fingerprints, której technologia bazuje na behawioralnym profilowaniu klientów i ich urządzeń. Rozwiązanie to wzbogaci ekosystem budowanych w BIK platform, służących do prewencji i wykrywania wyludzeń, dla

większego bezpieczeństwa instytucji i ich klientów, również poza sektorem finansowym.

POWIĘKSZA SIĘ RODZINA USŁUG ANTYFRAUDOWYCH BIK

Jak już wspominałem, dzięki startupowi Digital Fingerprints – twórcy rozwiązań z zakresu biometrii behawioralnej, powiększyła się rodzina usług antyfraudowych Biura Informacji Kredytowej. Dzięki temu do grupy już wdrożonych w BIK rozwiązań wykrywających fałszywe wnioski kredytowe w bankach (Platforma Antyfraudowa BIK) oraz systemu ochrony wszystkich transakcji online z poziomu weryfikacji urządzeń (Platforma Cyber Fraud Detection) dołącza kolejny innowacyjny mechanizm – biometria behawioralna.

To technologia, która pozwala weryfikować już nie tylko urządzenie, ale poddaje analizie zachowania użytkownika i sposób, w jaki danym urządzeniem się on posługuje. Pozwala wychwytywać oraz eliminować nieuprawnione transakcje, próby logowania czy zaciągnięcie nowych zobowiązań finansowych – wszystko to w czasie rzeczywistym.

„BACK TO FUTURE”

Futurystyczne wynalazki, jakie oglądaliśmy z zapartym tchem w kultowych filmach z lat 90. XX w., to rozwiązania, które obecnie należą do codzienności. Pewnie dziś uśmiechamy się, oglądając sceny z „Powrotu do przyszłości”. Nie było tam wzmianki o biometrii behawioralnej, bo to młoda technologia, która nawet teraz wydaje się abstrakcyjna. Niemniej innowacje, które pozostawały w sferze fikcji, obecnie stają się rzeczywistością.

Dzisiaj można bowiem stworzyć unikalny profil behawioralny, przypisany tylko jednej osobie na świecie, a więc niepodrabialny, który może służyć identyfikacji konkretnej osoby w momencie logowania się jej do konta czy to z komputera, czy z urządzenia mobilnego. To innowacja, która eliminuje dokonywanie oszukańczej operacji przez oszusta, np. nie dopuszcza do nieuprawnionego przelewu z konta albo złożenia wniosku kredytowego. Coraz częściej oszuści, wykorzystując socjotechniki, pozyskują dane klientów, niezbędne do logowania i do autoryzacji transakcji.

Dla przykładu, jeśli ktoś niepowołany posługuje się czyimiś danymi do logowania do banku, system powinien to wychwycić i ostrzec bank. Wówczas bank kontaktuje się z klientem, by poprosić o dodatkowe uwierzytelnienie.

WYZNACZANIE PROFILU BEHAVIORALNEGO

Biometria behawioralna bazuje na identyfikowaniu unikalnych zachowań człowieka. Z pomocą zaawansowanych obliczeń matematycznych i uczenia maszynowego, system przekształca zebrane dane, które „wypracowują” model zachowania użytkownika.

Profil behawioralny polega na połączeniu wielu czynników, którymi naturalnie posługujemy się, pracując na komputerze, tablecie czy smartfonie.

Prędkość pisania na klawiaturze, przerwy oraz tempo wciskania klawiszy, tworzą swego rodzaju „melodię pisania”. Szybkość poruszania myszką i sposób korzystania z urządzenia mobilnego

– wszystko to, dzięki odczytom z ekranu dotykowego i sensorów, poddane jest analizie niezbędnej do utworzenia unikalnego zachowania użytkownika i sposobu jego używania danego urządzenia.

Model behawioralny potrafi wychwycić anomalie w zachowaniu osoby korzystającej z urządzenia, co pozwala wykryć oszukańczą operację oraz ostrzec np. bank przed nieuprawnionym przelewem z konta albo złożeniem wniosku kredytowego. System niejako się przyucza – raz rozpoznany i wypracowany model behawioralny podlega systematycznemu uaktualnianiu. Z wiekiem, czy z upływem czasu, ludzkie zachowanie może się zmieniać, zatem również i model będzie się zmieniał razem z nami. To właśnie stanowi o przewadze profilu behawioralnego nad zwykłą biometrią, np. odcisk palca zapamiętuje się raz, bo nie zmienia się on w cyklu życia danego człowieka.

Warto podkreślić jeszcze jeden aspekt, ważny z perspektywy użytkowników w komunikacji z każdą instytucją. System profilowania zachowania klienta, choć dla niego samego jest niewidoczny, pozwala bezpiecznie i wygodnie go zidentyfikować. Podczas weryfikacji system nie sprawdza, co robi dany użytkownik, ale w jaki sposób to robi. Nie bada tego, co użytkownik wpisuje na klawiaturze, lecz to, jak z niej korzysta.

Zbierane informacje nie mają charakteru danych wrażliwych, są bezkontekstowe. Biometria behawioralna została uznana za metodę silnej autoryzacji klienta przez European Banking Authority. Banki, które skorzystają z tej technologii, nie muszą implementować innych mechanizmów autoryzacji, takich jak tokeny, SMS czy aplikacje mobilne. •

WIĘCEJ INFORMACJI:

- Digital Fingerprints – <https://fingerprints.digital/pl/>
- Biuro Informacji Kredytowej – <https://www.bik.pl/>

ŹRÓDŁA:

- Raport NetB@nk, IV kw. 2021 r., Związek Banków Polskich.
- Badanie „Cyberbezpieczeństwo Polaków 2022”, 30.03.2022 r., Quality Watch dla Biura Informacji Kredytowej, CAWI, 18+, N 1035,