Partnerzy raportu

BIK

GFT

INTEGRATED SOLUTIONS

technologie NASK

vsoft

CYFROWA TWIERDZA

Wydawcy raportu

Centrum Procesów Bankowych i Informacji
cpb.pl

BANK
MIESIĘCZNIK FINANSOWY

BANK.PL

Cyfrowa twierdza

Raport przygotowany przez
Centrum Procesów Bankowych i Informacji

Centrum Procesów Bankowych i Informacji
cpb.pl

Partnerzy raportu:
Biuro Informacji Kredytowej S.A.
Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy
GFT Poland Sp. z o.o.
Integrated Solution Sp. z o.o.
VSoft SA

Warszawa, grudzień 2023
Wydawnictwo Centrum Procesów Bankowych i Informacji

Spis treści

Cyberbezpieczeństwo banku
– aktualne trendy i wyzwania 4

Wiarygodność sztucznej inteligencji
fundamentem nowoczesnych
systemów cyberbezpieczeństwa 12

Biometria – najpewniejsza
metoda ochrony 20

Cyberbezpieczeństwo w erze chmury,
sztucznej inteligencji i szalonego tempa wdrożeń 24

Czy backup Twojego banku na pewno jest
adekwatny do zagrożeń? 28

Wewnątrzsektorowa wymiana informacji
i edukacja klientów to najskuteczniejsze
działania antyfraudowe 30

Cyberbezpieczeństwo banku – aktualne trendy i wyzwania

Przedstawiciele sektora bankowego od dawna zdają sobie sprawę z zagrożeń związanych z cyberatakami, jednak obecnie skala ekspozycji na ryzyko jest większa niż kiedykolwiek wcześniej. Zagrożenia dla cyberbezpieczeństwa szybko ewoluują, a cyberprzestępcy nieprzerwanie mają na celu system bankowy – z racji jego zasobności w aktywa finansowe.

Fot. Skórzewiak/stock.adobe.com

Fot. Archiwum prywatne

Dr hab. Grzegorz Strupczewski

PROFESOR UNIWERSYTETU EKONOMICZNEGO W KRAKOWIE. TRENER, ANALITYK ZAGROŻEŃ CYBERNETYCZNYCH I DOŚWIADCZONY WYKŁADOWCA AKADEMICKI. PASJONAT CYBERBEZPIECZEŃSTWA, W SZCZEGÓLNOŚCI JEGO ZAGADNIEŃ EKONOMICZNYCH I REGULACYJNYCH, TWÓRCA SZKOLEŃ TYPU CYBER AWARENESS. WYKONAWCA AUDYTÓW CYBERBEZPIECZEŃSTWA, EKSPERT W OBSZARZE DYREKTYWY NIS2 I NORMY ISO/IEC 27001. BADACZ RYZYK CYBERNETYCZNYCH, WYKONAWCA PROJEKTÓW NAUKOWYCH I BADAWCZO-WDROŻENIOWYCH. AUTOR KILKUDZIESIĘCIU PUBLIKACJI NAUKOWYCH, PRELEGENT NA KONFERENCJACH KRAJOWYCH I ZAGRANICZNYCH.
GRZEGORZ.STRUPCZEWSKI@UEK.KRAKOW.PL

Wstęp

Korzystanie z technologii teleinformatycznych (ICT) przez sektor bankowy odgrywa na tyle zasadniczą rolę, że obecnie ICT zyskały krytyczne znaczenie dla wykonywania typowych codziennych funkcji niemal wszystkich podmiotów finansowych i niefinansowych. Cyfryzacja obejmuje nie tylko płatności, ale także rozliczanie instrumentów finansowych, handel elektroniczny, operacje udzielania pożyczek i kredytów, finansowanie działalności gospodarczej, rating kredytowy, obsługę roszczeń i działalność back-office. Europejska Rada ds. Ryzyka Systemowego (ERRS) potwierdziła, że istniejący wysoki poziom wzajemnych powiązań między podmiotami finansowymi, różnymi rynkami i ich infrastrukturą, a szczególnie współzależności między systemami ICT, mogą stanowić podatność o charakterze systemowym. Istnieje obawa, że lokalne cyberincydenty mogą szybko się rozprzestrzeniać infekując cały system finansowy, bez względu na granice geograficzne[1].

Wyniki dwunastego corocznego badania EY/IIF *„Global bank risk management survey"*[2] z 2023 r. pokazują, że ryzyko cybernetyczne, wraz z ryzykiem kredytowym, jest traktowane przez CRO w bankach jako priorytetowe. Szczególnym wyzwaniem jest współzależność i nakładanie się wielu różnych ryzyk – tych typowych dla bankowości, jak i zupełnie nowych, o pochodzeniu wewnętrznym i zewnętrznym. Widać to wyraźnie na styku ryzyk geopolitycznego i cybernetycznego, które łącznie zagrażają cyfrowej od-

1 *„Cyberbezpieczeństwo. Zarys wykładu"*, pod red. Cezarego Banasińskiego, wyd. 2, Wyd. Wolters Kluwer, Warszawa 2023, s. 71.

2 https://www.ey.com/en_gl/banking-capital-markets/how-bank-cros-are-responding-to-volatility-and-shifting-risk-profiles

porności operacyjnej, jednocześnie zwiększając ryzyko rynkowe. Ryzyka te, pomimo swojej różnorodności, mają jedną wspólną cechę – za każdym razem wymagają natychmiastowej reakcji. Z kolei analizując potencjalne ryzyka w perspektywie najbliższych pięciu lat, wśród kluczowych wskazano zakłócenia spowodowane technologią, starzenie się systemów IT oraz prywatność danych. W zasadzie CRO dostrzegają ryzyko cybernetyczne wszędzie – w każdej linii biznesowej, w codziennych operacjach bankowych i projektach rozwojowych, a także u zewnętrznych partnerów i dostawców. Co warto podkreślić, 58% respondentów wskazało niezdolność do zarządzania ryzykiem cybernetycznym jako najważniejsze ryzyko strategiczne na najbliższe trzy lata.

Odpowiadając na wymogi Rozporządzenia DORA, które będzie stosowane od 17 stycznia 2025 r., banki poczyniły znaczące inwestycje w celu zwiększenia swojej cyfrowej odporności operacyjnej. Mechanizmy kontroli cyberryzyka zyskały najwyższy priorytet, a jako przykłady można wskazać procedury monitorowania i ograniczania cyberryzyka, budowę zaplecza technicznego oraz analizę zależności względem stron trzecich. Należy pamiętać, że ogólny poziom cyberbezpieczeństwa banku jest uzależniony od zaawansowania cyberhigieny i ochrony danych u partnerów zewnętrznych, którzy mogą stanowić najsłabsze ogniwo tego ekosystemu. Dlatego tak ważny jest dobór właściwej strategii współpracy – od okazjonalnego partnerstwa, poprzez zaangażowanie w joint ventures, a skończywszy na rozległej integracji i orkiestracji procesów biznesowych.

Banki jako cyfrowa twierdza o najwyższych standardach bezpieczeństwa

Banki, ze względu na charakter swojej działalności, są podatne na różne zagrożenia związane z cyberprzestępczością. Starając się na nie odpowiedzieć, w trosce o bezpieczeństwo swoich klientów i innych interesariuszy, stale doskonalą swoje systemy cyberbezpieczeństwa, w czym przypominają cyfrowe twierdze, oddzielone wysokimi murami od otoczenia i czyhających na nie niebezpieczeństw. Ta sytuacja wynika z szeregu okoliczności definiujących miejsce banków w ekosystemie społeczno-gospodarczym, do których należą:

- Dostęp do krytycznych danych: banki przechowują i przetwarzają duże ilości istotnych danych klientów, takich jak informacje finansowe i osobiste. Dlatego ochrona tych danych jest priorytetem.
- Rygorystyczne przepisy i regulacje: banki muszą przestrzegać rygorystycznych przepisów i regulacji dotyczących ochrony danych klientów i zapewnienia bezpieczeństwa transakcji finansowych. To sprawia, że są zobowiązane do spełnienia wysokich standardów bezpieczeństwa.
- Ataki hakerskie: banki są często celem zaawansowanych ataków hakerskich, takich jak APT, ransomware czy ataki DDoS. Muszą być przygotowane do reagowania na takie zagrożenia.
- Ciągła ewolucja zagrożeń: cyberprzestępczość jest dynamicznym obszarem, a zagrożenia ciągle ewoluują. Banki muszą być w stanie dostosować swoje środki ochrony do zmieniającej się sytuacji.
- Inwestycje w cyberbezpieczeństwo: banki zazwyczaj inwestują znaczne środki w technologie i zabezpieczenia związane z cyberbezpieczeństwem. Obejmuje to m.in. rozwijanie systemów ochrony przed atakami, monitorowanie ruchu sieciowego oraz szkolenia pracowników w zakresie świadomości dotyczącej zagrożeń.

Określanie banków jako cyfrowe twierdze to nie tylko trafna metafora, ale również odwołanie do znanego podejścia do budowania cyberbezpieczeństwa zwanego modelem twierdzy (ang. Castle Model). Model ten zakłada utworzenie mocnych i wieloaspektowych systemów obrony przed atakami cybernetycznymi. Jest to koncepcja, która wywodzi się z potrzeby zapewnienia maksymalnego poziomu bezpieczeństwa w obliczu stale zmieniających się zagrożeń w świecie cyfrowym. Wśród kluczowych aspektów modelu twierdzy można wymienić:

- Wielowarstwową ochronę: model twierdzy opiera się na zasadzie wielu warstw obrony (ang. Security in-depth). Oznacza to, że nie polega wyłącznie na jednym rodzaju zabezpieczenia, ale łączy wiele różnych mechanizmów i technologii, aby stworzyć kompleksową obronę.
- Prewencję i reakcje: model ten zakłada zarówno działania prewencyjne mające na celu uniknięcie ataku, jak i gotowość do reakcji w przypadku incydentu. To oznacza, że poza zapobieganiem, istotna jest również zdolność do szybkiego rozpoznania, reagowania i przywracania usług po ataku.
- Ciągły monitoring: kluczowym elementem modelu twierdzy jest ciągłe monitorowanie sieci i systemów w poszukiwaniu nieprawidłowości lub podejrzanych aktywności. Dzięki temu można wykryć ataki na wczesnym etapie.
- Edukację i świadomość: model ten zakłada, że pracownicy i użytkownicy systemów są kluczowym elementem ochrony. Dlatego istotne jest prowadzenie szkoleń i podnoszenie świadomości w zakresie cyberbezpieczeństwa.
- Partnerstwo i współpracę: twierdza w cyberbezpieczeństwie to także współpraca z innymi organizacjami, agencjami ds. cyberbezpieczeństwa oraz instytucjami rządowymi. Wspólna wymiana informacji i doświadczeń pomaga w identyfikacji nowych zagrożeń i skuteczniejszej obronie. →

Fot. Hanzala/stock.adobe.com

- Odporność i odzyskiwanie: model ten zakłada, że systemy powinny być odporne na ataki i gotowe do szybkiego odzyskiwania po incydencie. To obejmuje regularne tworzenie kopii zapasowych, procedury odzyskiwania danych i testowanie planów reagowania.
- Przestrzeganie przepisów i regulacji: organizacje wdrażające model twierdzy muszą przestrzegać restrykcyjnych przepisów i regulacji dotyczących cyberbezpieczeństwa, co zapewnia dodatkową warstwę ochrony.

Ze względu na postęp technologiczny, zmiany organizacyjne czy ewolucję interakcji człowiek-technologia, cyberbezpieczeństwo oparte na modelu twierdzy powinno być stale udoskonalane.

Postrzeganie banków jako cyfrowe twierdze znalazło odzwierciedlenie w opinii Polaków uczestniczących w cyklicznym badaniu „*Cyberbezpieczny portfel*" realizowanym przez Warszawski Instytut Bankowości we współpracy ze Związkiem Banków Polskich[3]. Respondenci uznali, że banki są liderami w zakresie cyberbezpieczeństwa, zdecydowanie wyprzedzając wojsko, policję, firmy technologiczne i inne grupy podmiotów. Uprawniony jest zatem wniosek, że banki – w oczach swoich klientów – dotrzymują kroku szybkiej digitalizacji i skutecznie odpowiadają na cyberwyzwania współczesności.

Cyberbezpieczeństwo banków – identyfikacja aktualnych trendów

Historycznie rzecz biorąc, banki działały jako izolowane podmioty. Funkcjonowały odrębne działy, każdy z unikalnymi celami, często korzystające z oddzielnych systemów. To fragmentaryczne podejście hamowało rozwój, ograniczało skalowalność i zmniejszało satysfakcję klientów. Wdrożenie ujednoliconej platformy, która centralizuje dane i wypełnia lukę między różnymi systemami, może skutecznie przeciwdziałać problemom, jakie stwarzają takie silosy. Jednak silosy informacyjne zwiększają również ryzyko naruszenia bezpieczeństwa danych i problemy związane z przestrzeganiem przepisów, wykraczające poza nieefektywność operacyjną, które są palącymi problemami w dzisiejszym ekosystemie bankowym. Integralność infrastruktury IT i ogromna ilość przechowywanych w niej danych pozostają głównymi problemami w procesie cyfrowej transformacji banków. Rozwiązanie problemu długu technologicznego ma kluczowe znaczenie. Dług ten jest często produktem ubocznym historycznych zaniedbań i zestawiania nowoczesnych technologii ze starszą infrastrukturą. Dawno minęły czasy, gdy bezpieczeństwo IT w bankowości miało charakter

3 https://zbp.pl/getmedia/bebff99e-f5b7-4644-aec-3-4ad3ff5c970a/Cyberbezpieczny_portfel_2022a

linearny. Dzisiejszy ekosystem bankowy składa się z dziesiątek, a nawet setek tysięcy wzajemnie połączonych urządzeń, od komputerów po urządzenia Internetu Rzeczy (IoT). A gdy uwzględni się kanały społecznościowe, chmurowe i mobilne, potencjalna powierzchnia ataku w przypadku naruszeń danych i zagrożeń cyberbezpieczeństwa rośnie wykładniczo. Pozostaje zatem palące pytanie. W jaki sposób banki mogą zapewnić bezpieczną sieć przy tak ogromnej złożoności? Jedną z możliwych odpowiedzi są wysoce skalowalne narzędzia cyberbezpieczeństwa i zarządzania ryzykiem działające w formule Software-as-a-Service (SaaS), a więc w modelu chmurowym.

Najlepszą taktyką obrony przed atakami jest zapobieganie im. Ci, którzy przygotują się na nadchodzące wyzwania, będą chronić ciągłość działania i reputację swoich organizacji – zwłaszcza, że cyberataki stają się coraz bardziej wyrafinowane. Liczba ataków związanych z nadużyciami finansowymi wykazuje tendencję wzrostową, a liczba cyberprzestępstw od 2013 r. niemal się potroiła. Intruzi intensyfikują wrogie działania, co jest stymulowane przez cyfryzację znacznej liczby usług bankowych. W miarę jak transakcje finansowe przechodzą do trybu online, rośnie liczba prób wyłudzeń. Co więcej, stale doskonalone są techniki cyberataków, a działalność przestępcza przeistacza się w model korporacyjny (Cybercrime-as-a-Service). Zorganizowane grupy przestępcze, jak i pojedyncze osoby mające dostęp do informacji zastrzeżonych wykorzystują nowatorskie technologie (np. uczenie maszynowe), aby uzyskać dostęp do aktywów bankowych. W odpowiedzi na wzrost ekspozycji na ryzyko cyfrowe banków powstają nowe regulacje prawne wprowadzające wysoko postawione wymagania w zakresie cyber security (Rozporządzenie DORA, Dyrektywa NIS2). Sprostanie im wiąże się ze znacznym wysiłkiem organizacyjnym i finansowym, eksponując jednocześnie rolę zarządzania ryzykiem cyfrowym i departamentów compliance w strukturze instytucji finansowych.

Banki podejmują odpowiednie działania, by zaadresować te wyzwania. Warto postawić na współpracę, gdyż wymiana danych o incydentach cybernetycznych oraz integracja narzędzi zapobiegawczych pomogą wzmocnić branżę. Partnerstwa publiczno-prywatne, edukacja klientów i kooperacja z dostawcami usług cyberbezpieczeństwa będą kształtować przyszłość cyberbezpieczeństwa w bankowości.

Najważniejsze zagrożenia bezpieczeństwa cyfrowego banków

W obecnym czasie banki muszą się mierzyć z szeregiem różnych zagrożeń cyfrowych, wśród których warto wymienić[4]:

- **Ataki APT (Advanced Persistence Threats)**. Zaawansowane trwałe zagrożenia (ataki APT) odnoszą się do zorganizowanych, szeroko zakrojonych kampanii, których celem jest ustanowienie długoterminowej, trudnej do wykrycia obecności w wewnętrznej sieci banku i przeprowadzenie dogłębnej infiltracji ofiary. Następnie intruzi systematycznie wykradają poufne dane oraz stopniowo przejmują kontrolę nad prawami dostępu do zasobów, dzięki czemu jeszcze bardziej poszerzają powierzchnię ataku. Do ataków APT wykorzystuje się trojany, backdoory oraz techniki służące do ukrycia obecności w systemie ofiary. Za ich wykonanie odpowiadają zorganizowane grupy przestępcze lub adwersarze działający na zlecenie rządów wrogo nastawionych państw trzecich.
- **Ataki na łańcuchy dostaw (Supply Chain attacks)**. Cyfryzacja bankowości umożliwia integrację wielu usług zewnętrznych z bezpiecznymi systemami bankowymi. Dla przykładu – rozwój oprogramowania dla branży fintech pozwolił neobankom uzyskać przewagę konkurencyjną w porównaniu z tradycyjnymi bankami. Takie zintegrowane usługi sieciowe oferują konsumentom wygodę obsługi. Z drugiej strony, rozwiązania te tworzą nowe podatności. Cyberprzestępcy mogą teraz atakować dostawców oprogramowania w łańcuchu dostaw, którzy mają słabsze zabezpieczenia. Przykładem może być firma Okta, która w październiku 2023 r. doświadczyła poważnej kradzieży danych spowodowanych atakami na łańcuch dostaw. Przestępcy włamali się do bibliotek z usługami uwierzytelniania za pośrednictwem repozytorium GitHub.
- **Phishing i inne ataki z wykorzystaniem inżynierii społecznej**. Niezmiennie najsłabszym, krytycznym punktem bezpieczeństwa IT w bankowości są ludzie. Przestępcy nadal wykorzystują socjotechniki, by nakłonić pracowników i klientów do podania swoich danych osobowych. Jest to jedna z form kradzieży tożsamości. Oszuści np. podają się za bank, przedstawicieli administracji lub nawet rządu w celu wyłudzenia danych kart kredytowych. Inni używają e-maili phishingowych lub wiadomości SMS zawierających złośliwe linki. Fałszywe strony internetowe, które naśladują legalne strony bankowe, to również często stosowane manipulacje. Kiedy Silicon Valley Bank trafił na pierwsze strony gazet z powodu zbliżającego się bankructwa, natychmiast wzrosła liczba fałszywych nazw domen z podobnymi adresami URL. Inżynieria społeczna we wszystkich swoich →

4 Na podstawie: *The State of Cybersecurity in Banking 2023*, EPAM, https://anywhere.epam.com/business/cyber-security-in-banking

formach pozostaje istotnym czynnikiem ryzyka, z którym powinien zmierzyć się zespół ds. cyberbezpieczeństwa.

- **Ataki ransomware**. Ransomware pozostaje głównym zagrożeniem dla bezpieczeństwa banków. Przestępcy kradną i szyfrują dokumenty finansowe, blokując klientom dostęp do ich własnych rachunków. W wielu przypadkach ataki ransomware mogą sparaliżować usługi bankowe na dłuższy czas. Aby odblokować usługi, należy zapłacić okup żądany przez przestępców. Ransomware pozostaje dużym problemem dla banków, ponieważ przestoje frustrują użytkowników i szkodzą reputacji instytucji. Przykładowo, w 2023 r. ransomware Lockbit przejął wewnętrzne operacje Banco de Venezuela, największej instytucji finansowej w Wenezueli.
- **Brak szyfrowania danych**. Hakerzy wkładają ogromny wysiłek w próby kradzieży danych w momencie, gdy pozostają one niezaszyfrowane na serwerze bankowym. W kwietniu 2023 r. badacze cyberbezpieczeństwa znaleźli niezaszyfrowaną bazę danych z poufnymi informacjami o klientach przechowywanymi przez kanadyjską platformę fintech NorthOne.
- **Nowe technologie jako źródło ryzyka**. Nowe technologie, takie jak sztuczna inteligencja, blockchain i kryptowaluty, stwarzają nowe ryzyka dla instytucji finansowych. Uczenie maszynowe i inteligentne kontrakty to przydatne i przełomowe rozwiązania dla tych, którzy mają dobrze przemyślaną strategię obrony. Obie technologie znajdują się na wczesnym etapie wdrażania, wciąż mają błędy w kodzie i podatności algorytmów, które inteligentni hakerzy próbują wykorzystać. Aktualizacja starszych systemów o nowe usługi jest dobrą praktyką, ale dopiero po przeprowadzeniu szeroko zakrojonej oceny ryzyka cyfrowego.
- **Luki w zabezpieczeniach chmury**. Branża bankowa stawia na rozwiązania chmurowe, które usprawniają wewnętrzne procesy operacyjne, jednak taka migracja wiąże się z ryzykiem. Co prawda dostawcy usług chmurowych oferują rozbudowane narzędzia kontroli bezpieczeństwa, ale mogą one okazać się bezużyteczne, jeśli zostaną źle skonfigurowane. Kluczowymi obszarami wpływającymi na bezpieczeństwo usług chmurowych są ochrona danych, zarządzanie dostępami i ryzyko nadużycia uprawnień.
- **Bezpieczeństwo urządzeń końcowych (endpoint security)**. Rozwój bankowości internetowej oraz mobilnej sprawił, że miliony urządzeń jej użytkowników, głównie komputerów i smartfonów, uzyskuje bezpośredni dostęp do cyfrowych usług finansowych. To sprawia, że bezpieczeństwo banku i zgromadzonych w nim środków jest uzależnione od przestrzegania zasad cyberhigieny przez pojedynczych klientów instytucji. Słabe hasła, brak szyfrowania i niewystarczające procesy uwierzytelniania zwiększają ryzyko związane z bezpieczeństwem sieci bankowych. Oszuści mogą wykorzystywać zgubione lub skradzione telefony, zbyt długie limity czasu wylogowania z konta w razie bezczynności użytkownika, nieaktualizowane oprogramowanie układowe (firmware) i nieefektywne zasady bezpieczeństwa urządzeń.
- **Zagrożenia wewnętrzne (insider threats)**. W tej kategorii znajdują się ryzyka wynikające z pracy zdalnej lub polityki BYOD (Bring Your Own Device). Zdalny dostęp jest trudny do monitorowania i wymaga nowych środków kontroli bezpieczeństwa. Szczególnie dotkliwe mogą być zaniedbania i nieostrożność pracowników przejawiająca się w przypadkowej infekcji złośliwym oprogramowaniem albo ujawnieniem wrażliwych danych osobom niepowołanym. Zorganizowane grupy przestępcze mogą próbować przekupić pracowników banku, by wykorzystując swoje uprawnienia i prawa dostępu do zasobów ułatwili przeprowadzenie ataku. Tak więc cyfryzacja procedur wewnętrznych zwiększa problem insider threats.
- **Dostęp zewnętrznych dostawców usług IT do wewnętrznej sieci banku**. Banki muszą przygotować się na zagrożenia cyfrowe związane z dostawcami zewnętrznymi. Instytucje finansowe polegają obecnie na zintegrowanych rozwiązaniach cyfrowych, a te relacje z vendorami wiążą się z ryzykiem. Oszuści mogą wykorzystywać słabe punkty mniejszych dostawców usług, aby uzyskać dostęp do sieci dużych banków. Podmioty trzecie reprezentują zróżnicowany poziom kultury cyberbezpieczeństwa, a banki w stosunku do nich mają niewielkie możliwości audytu bezpieczeństwa czy wpływu na poprawę sytuacji. Dostrzegając ten problem Unia Europejska uchwaliła Rozporządzenie DORA, które akcentuje problem ryzyka podmiotów trzecich kooperujących z instytucjami finansowymi. W podobnym kierunku zmierza Dyrektywa NIS2.

Warto dodać, że według raportu FAIR Institute „*Cybersecurity Risk Report 2024*"[5], najbardziej prawdopodobnymi scenariuszami cyberataków na instytucje finansowe będą:

- kradzież danych osobowych i finansowych przez pracownika banku (tzw. insider threat),
- eksfiltracja danych przez cyberprzestępców za pośrednictwem API dostarczonego bankowi przez partnerów zewnętrznych (tzw. atak na łańcuch dostaw),
- uzyskanie przez cyberprzestępców dostępu do systemu płatności i zlecanie sfałszowanych przelewów bankowych,

5 https://www.fairinstitute.org/2024-annual-cybersecurity-risk-report

Fot. TensorSpark/stock.adobe.com

- atak DDoS powodujący awarię krytycznych aplikacji bankowych dla klientów,
- atak ransomware na krytyczne aplikacje do przetwarzania transakcji powodujący awarię lub utratę danych.

Wzrost złożoności systemów cyberbezpieczeństwa zaczyna stanowić problem

Pomimo stałego wzrostu nakładów na cyberbezpieczeństwo, poziom zagrożenia ze strony cyberprzestępców stale rośnie wskutek stosowania nowoczesnych technologii i poszukiwania nowych wektorów ataku. Są tego świadomi menadżerowie wyższego szczebla odpowiedzialni za bezpieczeństwo informacji (CISO), wśród których jedynie 20% uważa, że poziom cyberbezpieczeństwa ich organizacji jest wystarczający w kontekście obecnych i przyszłych wyzwań[6]. Według raportu „*EY 2023 Global Cybersecurity Leadership Insights Study*", organizacje doświadczają średnio 44 poważnych incydentów cybernetycznych rocznie. Przewiduje się, że koszty ataków ransomware wzrosną z 20 mld USD w 2021 r. do 265 mld USD w roku 2031[7]. Tymczasem nakłady na cyberbezpieczeństwo rosną w średniorocznym tempie 16,6% (EY 2023).

Cytowany wcześniej raport EY (2023) zwraca uwagę na zaskakujący paradoks. Otóż skala i złożoność narzędzi bezpieczeństwa IT może stanowić największe zagrożenie dla skuteczności polityki cyberbezpieczeństwa ze względu na problem szumu informacyjnego, a więc ograniczonej transparentności ogromu danych, sygnałów, alertów generowanych przez różne urządzenia. Rozwiązaniem tego problemu może być integracja zadań na jednej platformie i agregacja danych. Potrzebna jest holistyczna technologia cyberbezpieczeństwa i racjonalizacja procesów wewnątrz organizacji. W szczególności należy zwrócić uwagę na implementację takich technologii, jak: sztuczna inteligencja (AI) i uczenie maszynowe (ML), uwierzytelnienie bez użycia haseł (paswordless authentication), automatyzacja i orkiestracja usług chmurowych, robotyzacja procesów, systemy SOAR (Security Orchestration, Automation and Response). Przedstawione podejście do cyberbezpieczeństwa można określić jako „bezpieczeństwo dzięki prostocie" (security through simplification). Autorzy raportu EY 2023 przekonują organizacje o wysokim stopniu rozwoju kultury cyberbezpieczeństwa, a do takich bez wątpienia zaliczają się banki, do implementacji podejścia „security →

6 EY 2023 Global Cybersecurity Leadership Insights Study, https://www.ey.com/en_gl/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy

7 Cybersecurity Ventures (2023), https://cybersecurityventures.com/cybersecurity-almanac-2022/

through simplification". Może to doprowadzić do szeregu korzyści, takich jak:

- Obniżenie całkowitego kosztu posiadania zasobów IT (Total Cost of Ownership) i zwiększenie tempa realizacji procesów wewnętrznych dzięki uproszczeniu i racjonalizacji istniejących rozwiązań cyberbezpieczeństwa.
- Eliminacja przestarzałych systemów, które powielają się lub są słabo zintegrowane z bardziej nowoczesnymi rozwiązaniami.
- Uproszczenie i automatyzacja procesów cyberbezpieczeństwa poprzez redukcję liczby niezależnych konfiguracji.
- Rozwój własnych zdolności przeciwdziałania zagrożeniom bez jednoczesnego zwiększania złożoności środowiska technologicznego.
- Uproszczenie infrastruktury IT i podniesienie efektywności kosztowej dzięki wdrożeniu podejścia opartego na usługach zarządzanych (managed services) i tzw. co-sourcingu (co-sourcing to model współpracy organizacji z zewnętrznymi dostawcami usług IT, gdzie korzysta się z zasobów i kompetencji zewnętrznego dostawcy przy zachowaniu pewnej kontroli nad własnymi procesami i zasobami wewnętrznymi).

W ostatnim czasie poważnym wyzwaniem dla cyberbezpieczeństwa organizacji jest zwiększenie potencjalnych powierzchni ataku. Wynika to z powszechnego wykorzystania chmury oraz urządzeń Internetu Rzeczy (IoT), a także nieodpowiednio zabezpieczonych elementów łańcucha dostaw. W efekcie stopniowo zanika granica oddzielająca wewnętrzną infrastrukturę IT organizacji od otoczenia. W dotychczas obowiązującym podejściu do cyberbezpieczeństwa, zwanym modelem twierdzy, ochrona tej granicy stanowiła jeden z fundamentów polityki bezpieczeństwa.

Zwiększenie powierzchni ataków nie jest jedynym wyzwaniem cyberbezpieczeństwa dla banków i innych dużych organizacji. Wśród potencjalnych zagrożeń wymienia się (EY 2023):

- Trudność w znalezieniu równowagi między bezpieczeństwem a wysokim tempem wdrażania innowacji.
- Lekceważenie zasad cyberhigieny przez pracowników nietechnicznych.
- Niewystarczające przygotowanie organizacji na nowo powstające cyberzagrożenia.
- Nieadekwatny do potrzeb i ekspozycji na ryzyko budżet na cyberbezpieczeństwo,
- Postrzeganie cyberbezpieczeństwa wyłącznie jako zadania dla działów IT.

Raportowanie ryzyka cybernetycznego wewnątrz organizacji

Budowa bezpiecznego ekosystemu bankowego, odpornego na zagrożenia cybernetyczne, powinna uwzględniać nie tylko rozwiązania IT, ale także raportowanie cyberryzyka, co ma kluczowe znaczenie dla skutecznego, opartego na rzetelnych danych procesu zarządzania ryzykiem. Jak dowodzi PwC[8], wiele organizacji ma problem z odpowiedzią na tak podstawowe pytania, jak: które zasoby powinny być chronione, jakie dane dotyczące ekspozycji na cyberryzyko są najistotniejsze i należy je gromadzić, jaki może być prawdopodobny wpływ incydentu cybernetycznego na ciągłość procesów biznesowych. Nie dysponując takimi informacjami, trudno o przeprowadzenie rzetelnej analizy kosztów i korzyści z inwestycji w poprawę cyberbezpieczeństwa. Efektywne raportowanie ryzyka cybernetycznego pomaga kluczowym interesariuszom, takim jak zarząd i organy regulacyjne, uzyskać pewność co do racjonalności podejmowanych decyzji w obszarze *cybersecurity*. Ponadto warto zwrócić uwagę, że zagrożenia cybernetyczne wpływają na wiele różnych obszarów organizacji. Przykładowo, ochrona infrastruktury IT i zwiększanie bezpieczeństwa cyfrowego ma przełożenie na strategiczne decyzje w obszarze ESG.

Zbudowanie efektywnego systemu pomiaru i raportowania cyberryzyka powinno opierać się na kilku kluczowych zasadach, takich jak: model ryzyka powinien umożliwiać automatyzację i bieżącą aktualizację przy odpowiednim poziomie elastyczności we wdrażaniu modyfikacji; prezentacja aktualnych danych o ryzyku na interaktywnych i czytelnych dashboardach; odejście od raportowania każdego wskaźnika i skupienie się na tych kluczowych; przekaz syntetycznej informacji dla zarządu; powiązanie alertów o incydentach z danymi o zagrożeniach, powierzchni ataku, metrykach ryzyka oraz zdolnościach organizacji do mitygacji ataku. Warto również powiązać powyższe informacje z bieżącymi projektami cyberbezpieczeństwa celem ustalenia priorytetów inwestycji w cybersecurity.

Sztuczna inteligencja

McKinsey przewiduje, że sztuczna inteligencja będzie miała istotny wpływ stymulujący na produktywność w różnych branżach gospodarki, na czele z sektorem bankowym. Zdaniem autorów raportu „*The economic potential of generative AI: The next productivity frontier*", bankowość należy do branż, które mogą odczuć największy pozytywny wpływ sztucznej inteligencji zyskując dodatkowe 200–340 mld USD przychodów rocznie, co stanowi 3–5% rocznych przychodów całego sektora bankowego[9]. Do

8 PwC (2023), *Starting on the journey to data-driven cyber risk reporting*, https://www.pwc.co.uk/issues/cyber-security-services/insights/data-driven-executive-cyber-risk-reporting.html

9 McKinsey (2023), *The economic potential of generative AI: The next productivity frontier*, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#key-insights

największych korzyści z wykorzystania AI w bankowości można zaliczyć (McKinsey 2023):

- W obszarze inżynierii oprogramowania – konwersja przestarzałego kodu w aplikacjach bankowych (optymalizacja migracji ze starszych frameworków dzięki możliwościom tłumaczenia na język naturalny).
- W obszarze obsługi klienta – obsługa interaktywnych połączeń głosowych z klientami (IVR – Interactive Voice Response), zautomatyzowane, szybsze i bardziej kompleksowe rozwiązywanie problemów klientów za pośrednictwem systemu IVR wspomaganego przez AI (np. kompleksowa obsługa zgłoszeń utraty kart płatniczych).
- W obszarze marketingu i sprzedaży – generowanie spersonalizowanych ofert produktów w bankowości detalicznej na podstawie profilu klienta i historii współpracy z danym bankiem.
- W obszarze operacyjnym – zautomatyzowane tworzenie dokumentacji stosowanych modeli zarządzania ryzykiem, a także weryfikacja kompletności posiadanej dokumentacji w kontekście wymogów regulacyjnych.

Wykorzystanie narzędzi sztucznej inteligencji może zwiększyć zadowolenie klientów, usprawnić podejmowanie decyzji, poprawić user experience (UX) pracowników oraz zmniejszyć ryzyko banku poprzez lepsze monitorowanie oszustw i nadużyć. Bankowość, jako dziedzina oparta na wiedzy i technologii, odniosła już znaczne korzyści z wcześniejszych zastosowań sztucznej inteligencji w obszarach takich, jak marketing i obsługa klienta. Generatywne wdrożenia sztucznej inteligencji mogą przynieść dodatkowe korzyści, zwłaszcza że duże modele językowe LLM doskonale nadają się do wykorzystania w takich obszarach, jak regulacje i programowanie.

Specyficzne cechy charakteryzujące sektor bankowości sprawiają, że jest to branża w szczególny sposób predestynowana do czerpania ponadprzeciętnych korzyści z wykorzystania AI. Można tu wymienić m.in. (McKinsey 2023):

- Zaawansowane prace na rzecz cyfryzacji przy jednoczesnym istnieniu starszych systemów informatycznych. Banki inwestują w technologię od dziesięcioleci, akumulując znaczący dług technologiczny wraz z silosową i złożoną architekturą IT.
- Duża liczba pracowników mających bezpośredni kontakt z klientem. Bankowość opiera się na dużej liczbie pracowników sprzedażowych, doradcy klienta w oddziałach banku lub call-center.
- Rygorystyczne środowisko regulacyjne. Jako branża silnie regulowana, bankowość ma znaczne potrzeby w zakresie zarządzania ryzykiem i zapewnienia zgodności z prawem (compliance).
- Branża pracowników umysłowych. Wpływ sztucznej inteligencji może objąć całą organizację, pomagając wszystkim pracownikom w pisaniu e-maili, tworzeniu prezentacji biznesowych i innych tego typu zadaniach.

Podsumowanie

Zarządzanie ryzykiem cybernetycznym we współczesnej bankowości wykracza poza środki techniczne i obejmuje holistyczne podejście obejmujące całą organizację. Wiele instytucji boryka się jednak z ograniczonymi narzędziami do oceny zagrożeń dla cyberbezpieczeństwa, zwłaszcza podczas integracji z nowymi partnerami i technologiami. Najnowsze regulacje, takie jak DORA, kładą nacisk na odporność operacyjną, opowiadając się za globalnie dostosowanymi ramami zarządzania ryzykiem. Ta międzynarodowa konwergencja ma na celu standaryzację praktyk i zmniejszenie fragmentacji. Godnym uwagi aspektem tych przepisów jest kontrola dostawców zewnętrznych, biorąc pod uwagę ich rosnące znaczenie w ekosystemie finansowym. Chociaż banki są tradycyjnie ostrożne w wyborze dostawców IT, rozwój innowacyjnych startupów oferuje szereg obiecujących rozwiązań. Tą otwartość należy starannie wyważyć z uwagi na ryzyko potencjalnych luk bezpieczeństwa u podmiotów trzecich. W miarę cyfrowej ewolucji banków zharmonizowane podejście do zarządzania ryzykiem, które uwzględnia globalne regulacje i integrację z podmiotami zewnętrznymi, ma kluczowe znaczenie dla bezpieczeństwa i rozwoju sektora bankowego.

Chociaż sektor bankowy jest wzorem stabilności finansowej, w coraz większym stopniu zmaga się z podwójnymi wyzwaniami – zapewnieniem solidnego cyberbezpieczeństwa i dostosowaniem do wciąż zmieniających się przepisów. Banki, chcąc sprostać wymaganiom klientów i przeciwdziałać zagrożeniom cyberbezpieczeństwa, jednocześnie poruszają się w labiryncie rygorystycznych przepisów dotyczących prywatności i bezpieczeństwa danych. Te środki regulacyjne, w połączeniu z coraz bardziej złożonym krajobrazem cyberzagrożeń, spowodowały wzrost kosztów operacyjnych, szczególnie w obszarze compliance, zarówno w przypadku banków detalicznych, jak i korporacyjnych.

Od dłuższego czasu sektor bankowy zalicza się do liderów innowacji technologicznych i cyfrowych, dlatego kluczowe znaczenie będzie mieć znalezienie równowagi między innowacjami, zagrożeniami dla cyberbezpieczeństwa i zgodnością z przepisami. Właściwe skomponowanie tej triady może odblokować potencjał rozwojowy, zapewniając wejście na bezpieczną, zgodną z regulacjami i dochodową ścieżkę wzrostu. •

Wiarygodność sztucznej inteligencji fundamentem nowoczesnych systemów cyberbezpieczeństwa

NASK technologie NASK

Coraz bardziej złożone i urozmaicone ataki cybernetyczne stanowią nowe wyzwania dla sektora bankowego. W walce z cyberprzestępczością rola sztucznej inteligencji (SI) staje się kluczowa. Wykorzystując SI, systemy cyberbezpieczeństwa mogą analizować ogromne ilości danych w czasie rzeczywistym, identyfikując wzorce, anomalie i co za tym idzie, potencjalne zagrożenia. Jednakże, w parze z poziomem zaawansowania i dokładnością predykcji dokonywanych przez te systemy nie zawsze idzie ich wiarygodność. Problem ten jest szczególnie istotny w bankowości, gdzie zaufanie klientów jest kluczowe.

Mateusz Krzysztoń
Kamila Lis
Andrzej Sikora
Przemysław Jaskóła
NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA
PAŃSTWOWY INSTYTUT BADAWCZY

Wstęp

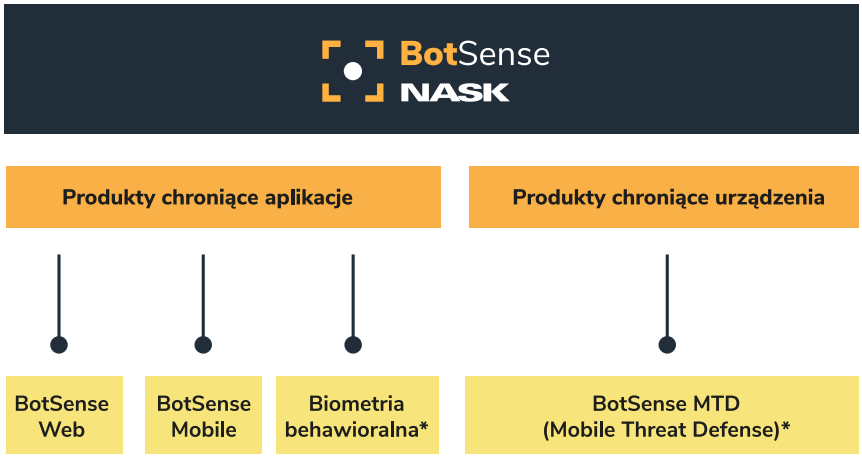
Budowanie wiarygodnych systemów SI oraz weryfikacja ich rzetelności jest bardziej złożona niż w tradycyjnych systemach cyberbezpieczeństwa. Podczas gdy tradycyjne systemy cyberbezpieczeństwa opierają się na wiedzy eksperckiej, systemy SI korzystają z algorytmów zdolnych do adaptacji i samodzielnej nauki. Działają w oparciu o dane, które mogą być różnej jakości, stąd popularne w społeczności SI powiedzenie odnoszące się do wpływu jakości danych na wynikowy system – „*Garbage in, garbage out*".

Zależność od danych, jak również dynamiczna natura modelowanych zjawisk (np. wektorów ataków), sprawia, że aspekty związane z wiarygodnością nabierają zupełnie nowego wymiaru. W dziedzinie systemów tradycyjnych istnieje szereg sprawdzonych metodyk oraz dobrych praktyk dotyczących wytwarzania systemu, jak również kryteriów weryfikacji poszczególnych jego aspektów, które składają się na ostateczną ocenę wiarygodności. Natomiast w kontekście systemów sztucznej inteligencji prace w tych obszarach wciąż trwają. Dostępnych jest wiele technik i narzędzi, które mogą służyć do określania wiarygodności takich systemów. Choć część z nich jest jeszcze daleka od osiągnięcia pełnej dojrzałości, to z pozostałych można już korzystać.

W naszych projektach wiarygodność sztucznej inteligencji uznajemy za fundament nowoczesnych systemów cyberbezpieczeństwa. Dla lepszego zobrazowania przykładowych aspektów wiarygodności systemów SI poniżej omówimy je na przykładzie trzech rozwiązań realizowanych w NASK w ramach grupy

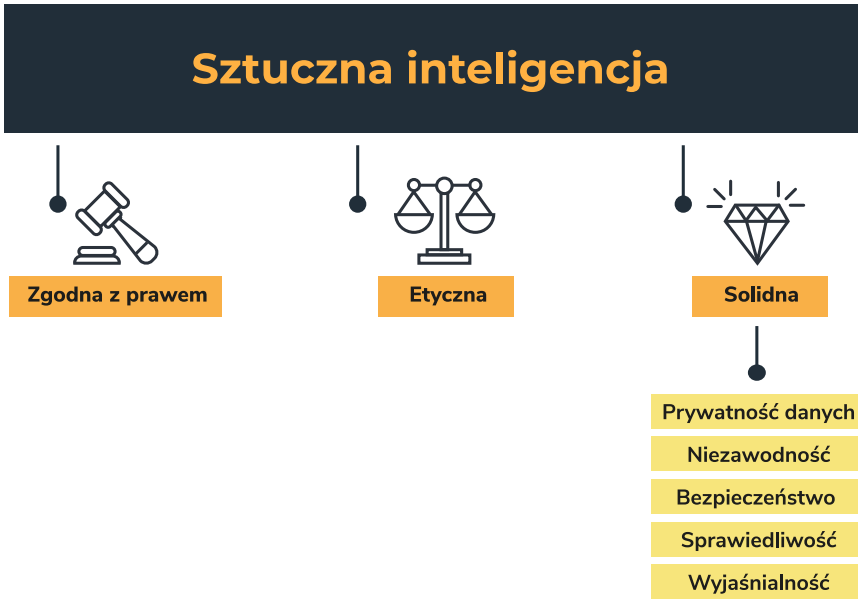
produktów BotSense. BotSense jest systemem służącym do wykrywania aktywności złośliwego oprogramowania w urządzeniach użytkowników bankowości elektronicznej i mobilnej. W ramach BotSense sztuczna inteligencja wykorzystywana jest do poprawy bezpieczeństwa użytkowników w wieloraki sposób. Na urządzeniach Android moduł Malware Hunter AI (wchodzący w skład produktów BotSense Mobile i BotSense MTD) wykrywa złośliwe aplikacje, które nie zostały jeszcze zidentyfikowane i umieszczone w bazach malware. Użytkowników bankowości elektronicznej korzystających z przeglądarki chronią m.in. moduł Remote Checker, a już niedługo również komplementarny do niego moduł biometrii behawioralnej. Pierwszy z nich sprawdza, czy przeglądarka użytkownika nie jest przechwycona przez atakującego za pośrednictwem oprogramowania zdalnego pulpitu, natomiast drugi poprzez analizę behawioralną dodatkowo weryfikuje tożsamość klientów banku na podstawie ich interakcji z aplikacją banku.

Ilustracja 1. Grupa produktów BotSense



*Produkt obecnie w fazie wdrożenia.

Ilustracja 2. Filary wiarygodności systemów SI



1. Wiarygodność SI

Wiarygodność systemów sztucznej inteligencji opiera się na trzech filarach: legislacji, etyce oraz solidności. Pierwszy filar, legislacja, odnosi się do działania w granicach obowiązującego prawa. Natomiast w obszarach, gdzie prawo nie nadąża za postępem technologicznym, kluczowy staje się drugi filar – etyka, która obejmuje respektowanie przyjętych społecznie norm, takich jak m.in. szacunek dla prywatności oraz uczciwość wobec użytkowników.

Ostatni filar, solidność, dotyczy technicznych zagadnień tworzenia systemów. Jego celem jest zapewnienie, by system działał zgodnie z oczekiwaniami, niezawodnie, bezpiecznie, sprawiedliwie, a także by był transparentny i gwarantował bezpieczeństwo danych – zarówno tych wykorzystywanych do tworzenia systemu, jak również tych pochodzących od zabezpieczanych klientów banku.

Skupiając się na technicznej stronie wiarygodności SI, posłużymy się kilkoma przykładami w pięciu podstawowych aspektach solidności: bezpieczeństwie danych, niezawodności, odporności na cyberataki, sprawiedliwości i wyjaśnialności.

a. Bezpieczeństwo danych

W systemach SI konieczne jest zapewnienie prywatności przetwarzanych danych użytkownika. Najczęściej, by wytrenować model uczenia maszynowego, niezbędne jest przesłanie danych użytkowników na serwer, na którym model jest uczony. Takie rozwiązanie może nie odpowiadać preferencjom klienta, dodatkowo może stanowić zagrożenie dla jego prywatności w przypadku wycieku danych. Jednym z potencjalnych rozwiązań tego problemu jest podejście, w którym z urządzenia →

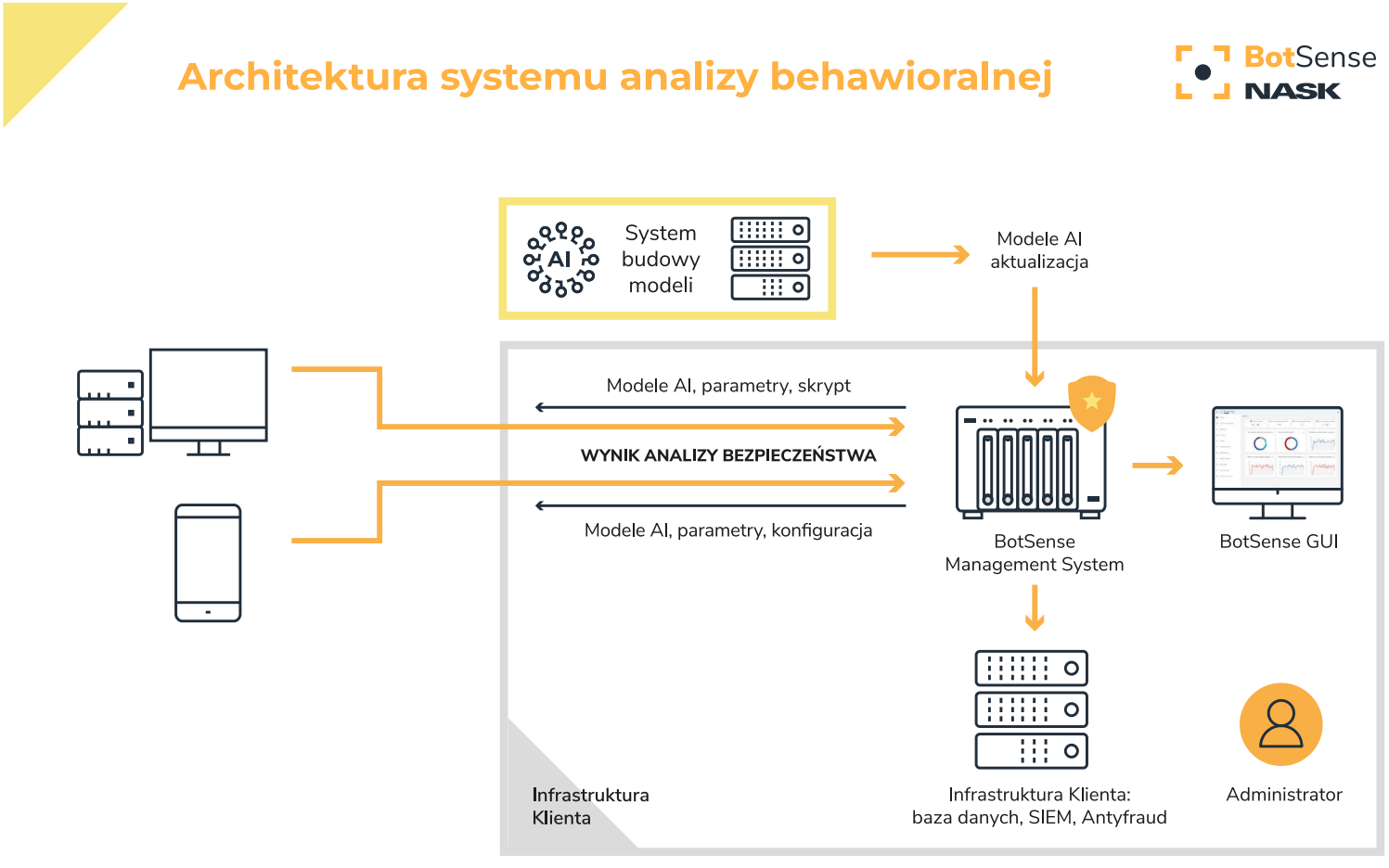
użytkownika są przesyłane jedynie gradienty, uwzględniane do poprawy modelu. Na przykładzie jednokierunkowej sieci neuronowej udowodniono jednak, że odtworzenie oryginalnych danych z wiadomości przesyłanych do serwera jest możliwe, zatem rozwiązanie to nie zapewnia pełnej prywatności danych.

Innym sposobem na uniknięcie przesyłania i przetwarzania danych użytkownika poza jego urządzeniem jest zastosowanie lekkich modeli sztucznej inteligencji. Modele te charakteryzują się mniejszą liczbą parametrów uczenia, co pozwala na uruchomienie ich na urządzeniu końcowym. W tym podejściu dane nie opuszczają urządzenia użytkownika, ponieważ wszystkie predykcje obliczane są na jego urządzeniu. W ten sposób lekka SI pozwala na zwiększenie bezpieczeństwa użytkownika przy jednoczesnym poszanowaniu prywatności jego danych. Dodatkowo koszty operacyjne związane z wdrożeniem i utrzymaniem lekkiego rozwiązania są niższe.

Lekkie modele są wdrażane również jako nowe moduły systemu BotSense. Jednym z modułów jest Remote Checker – narzędzie umożliwiające detekcję prób przejęcia sesji użytkownika z wykorzystaniem oprogramowania zdalnego pulpitu. Moduł ten wykorzystuje szereg przesłanek charakterystycznych dla sytuacji, w której atakujący zdalnie steruje kursorem myszy w przeglądarce atakowanego. Moduł ten analizuje m.in. dynamikę ruchu kursora. Zbierane dane są potencjalnie danymi wrażliwymi, gdyż mogą posłużyć do budowy profilu behawioralnego użytkownika. Dzięki zastosowaniu lekkiej architektury SI dane te nie opuszczają przeglądarki.

Również moduł biometrii behawioralnej oraz moduł Malware Hunter AI dostępne będą w wersji lekkiej.

Ilustracja 3. Architektura systemu analizy behawioralnej



„Zastosowanie lekkiej SI działającej wyłącznie lokalnie w przeglądarce użytkownika zapewnia poufność wrażliwych danych”.

b. Niezawodność

Niezawodność systemu sztucznej inteligencji odnosi się do jego zdolności do skutecznego wykonywania zadań w różnych warunkach i sytuacjach. Dotyczy to nie tylko poprawnego działania w przewidzianych scenariuszach, ale także odporności na niespodziewane wyzwania i zakłócenia. Na wysoką niezawodność systemu składają się przede wszystkim wysokiej jakości dane, poprawny proces wytworzenia systemu oraz monitorowanie jego pracy po wdrożeniu.

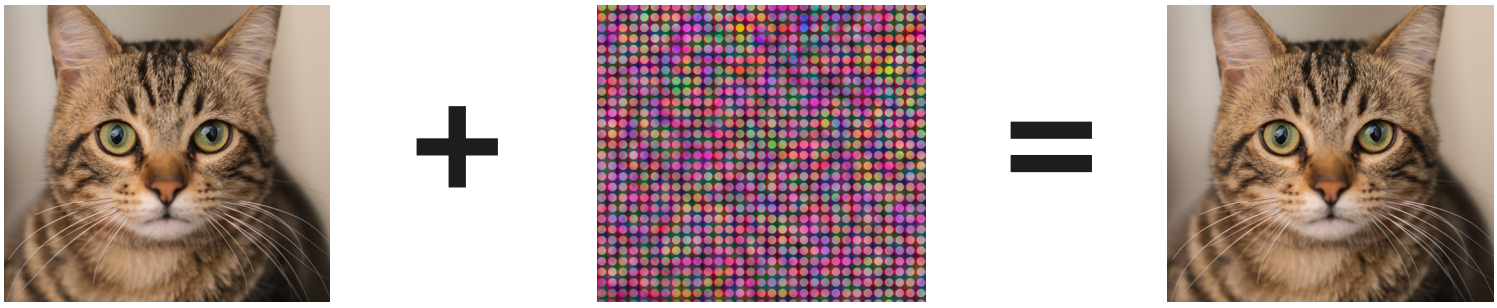
Składnikiem niezawodności systemu, odpowiednio zwiększającym również jego transparentność, jest obszerne raportowanie, w ramach dokumentacji systemu, wyników osiągniętych na różnych zbiorach danych, które mogą być reprezentatywne, np. dla różnych grup klientów. Twórców – w poprawnej dokumentacji systemu, a odbiorców – w zrozumieniu dostarczanej dokumentacji, wspierają odpowiednie standardy opracowywane przez międzynarodowe grupy ekspertów. I choć w przypadku SI prace w tych grupach wciąż trwają, to pierwsze dokumenty mogą być już z powodzeniem stosowne – np. w ramach Malware Hunter AI obszerne raportowanie wskaźników wykorzystuje metryki zawarte w specyfikacji technicznej ISO/IEC TS 4213.

Innym czynnikiem składającym się na niezawodność jest odpowiednie monitorowanie działania systemu. Choć systemy SI uczą się na danych historycznych, chcemy by zachowywały wysoką skuteczność na nowych danych. Jednak zmiana charakteru obserwowanego zjawiska (przykładowo, pojawienie się nowej rodziny malware) może powodować pogorszenie jakości systemu. Do monitorowania tej zmienności obserwowanego zjawiska, zwanego dryftem, można stosować np. narzędzie NannyML. Gdy dryft jest znaczący, konieczne może być przeuczenie systemu na nowych danych. Posiadanie odpowiednio zaprojektowanego procesu monitorowania daje pewność co do rzeczywistej jakości działania systemu SI i pozwala podjąć z wyprzedzeniem odpowiednie środki zaradcze.

c. Odporność na ataki

Innym istotnym aspektem wiarygodności systemów ML jest odporność na ataki. Poprawne działanie w warunkach wrogich jest z oczywistych względów szczególnie istotne w przypadku systemów cyberbezpieczeństwa. Istnieje wiele typów ataków specyficznych dla systemów ML, na które tradycyjne systemy nie są podatne. Modele SI mogą działać na zasadzie „czarnych skrzynek”, co sprawia, że atakujący są w stanie eksplorować niezrozumiałe dla człowieka obszary w procesie decyzyjnym, znajdując lukę →

Ilustracja 4. Atak unikania na system klasyfikacji obrazów. Do zdjęcia poprawnie klasyfikowanego przez system SI dodawane jest zaburzenie niewidoczne dla człowieka. W efekcie system SI przestaje poprawnie klasyfikować obraz



w wiedzy systemu. Ten typ ataku nazywany jest atakiem unikania. Ilustracja nr 4 przedstawia idee ataku unikania – atakujący znajduje zakłócenie, które jednocześnie jest niezauważalne dla obserwatora i powoduje oszukanie systemu SI.

Choć najczęściej atak ten jest rozważany w przypadku obrazów, jest on również możliwy do zastosowania w innych obszarach, np. w przypadku systemu do detekcji malware. Tu celem atakującego jest wprowadzenie tak nieznacznej manipulacji do aplikacji złośliwej, by nie naruszyć jej złośliwej funkcjonalności, a jednocześnie sprawić, by system antywirusowy rozpoznał ją jako łagodną.

Inną grupą ataków jest zatruwanie danych trenujących wykorzystywanych do budowy wiedzy systemu. Jednym z ataków z tej grupy jest atak „tylnych drzwi" (ang. *backdoor*) polegający na wstrzyknięciu przez atakującego do zbioru trenującego próbek z tzw. triggerem – charakterystyczną kombinacją wartości, które determinują późniejsze zachowanie modelu. Posługując się ponownie przykładem systemu do detekcji aplikacji złośliwych, atakujący może wprowadzić trigger do aplikacji łagodnych wykorzystywanych w procesie trenowania. W ten sposób system może nauczyć się, że obecność triggera świadczy o łagodności aplikacji. Jak łatwo się domyślić, umieszczenie takiego triggera w aplikacji złośliwej może pomóc w oszukaniu systemu sztucznej inteligencji.

Istnieją na szczęście metody obrony przed tym rodzajem ataków. W przypadku modułu Malware Hunter AI jednym z przeciwdziałań jest wybór takich cech opisujących aplikacje mobilne, które są najmniej wrażliwe na ataki „tylnych drzwi". Natomiast w module biometrii behawioralnej wzorce zachowania użytkownika są zapisywane jako reprezentacja pośrednia (tzw. *embedding*), która jest niezrozumiała dla atakującego. Nawet znalezienie embeddingu kompromitującego system SI nie daje jeszcze atakującemu wiedzy o oryginalnym wzorcu, a operacja odwrócenia embeddingu jest procesem trudnym.

d. Sprawiedliwość

W kontekście systemów decyzyjnych sprawiedliwość oznacza brak faworyzowania lub uprzedzeń wobec danej jednostki lub grupy na podstawie jej wrodzonych lub nabytych cech. Jest to dążenie do równego traktowania wszystkich, niezależnie od ich charakterystyk. Koncepcja sprawiedliwości wiąże się również z pojęciem stronniczości (ang. *bias*) w systemach SI. Stronniczość definiuje się jako negatywne i niepożądane skutki działania tych systemów, szczególnie jeśli skutki te dotykają określone grupy ludzi w sposób nieproporcjonalny.

Typowym przykładem w dziedzinie bankowości, gdzie uprzedzenie systemów SI może dać o sobie znać, są systemy oceny zdolności kredytowej, które mogą mieć tendencję do obniżania wskaźnika osobom np. przynależącym do określonej grupy etnicznej tylko z uwagi na tę przynależność przy braku innych przesłanek. Inaczej mówiąc, z niedozwoloną stronniczością systemu mamy do czynienia w sytuacji, gdy ten system nieproporcjonalnie częściej popełnia błąd na niekorzyść jednej z grup.

Również w systemach cyberbezpieczeństwa konieczne jest zwrócenie uwagi na sprawiedliwość systemu, zwłaszcza jeśli system ten może decydować np. o utrudnieniu dostępu do konta klientów banku. Przykładowo, w ramach analizy behawioralnej i modułu oceniającego sposób wpisywania loginu przez użytkownika, można spodziewać się, że osoby starsze mogą pisać wolniej na klawiaturze. Dlatego na etapie zbierania danych treningowych i testowych konieczne jest zidentyfikowanie grup użytkowników, dla których spodziewamy się, że charakterystyka danych może się różnić (np. ze względu na wiek, częstość korzystania z urządzeń elektronicznych) i zadbanie, by nasze dane były reprezentatywne, a wytworzony system SI równie skuteczny we wszystkich podgrupach.

e. Wyjaśnialność

Jedną z najczęściej podnoszonych wad sztucznej inteligencji, wpływających na wiarygodność systemu, jest ograniczona zdolność do wyjaśnienia, dlaczego systemy SI podejmują konkretne decyzje. W zależności od typu algorytmu uczenia wykorzystanego do realizacji systemu, system ten charakteryzuje się innym stopniem wyjaśnialności swoich decyzji. Choć stopień ten jest odmienny dla każdego algorytmu uczenia, w ogólności modele ML można podzielić na dwie grupy: modele interpretowalne i modele wytłumaczalne. Najprościej różnicę między tymi pojęciami można ująć następująco: modele wytłumaczalne mogą być zrozumiane przez człowieka tylko z wykorzystaniem dodatkowych technik, natomiast do zrozumienia modeli interpretowalnych wystarczy poznanie ich budowy i parametrów.

Przykładem w pełni interpretowalnego modelu jest drzewo decyzyjne, gdzie każdy węzeł reprezentuje konkretne kryterium decyzyjne, a każdy liść oznacza finalną decyzję. W drzewie decyzyjnym proces podejmowania decyzji jest łatwy do zrozumienia, ponieważ można prześledzić ścieżki od korzenia do liści, a każdy etap jest jasno interpretowalny. Na drugim biegunie pod względem wyjaśnialności znajdują się sieci neuronowe, w przypadku których interpretowalność staje się wyzwaniem. Sieci neuronowe uczą się skomplikowanych zależności i cech,

które mogą być trudne do zrozumienia nawet dla specjalistów, a model pozostaje „czarną skrzynką".

Należy jednak zaznaczyć, że coraz większą popularność zdobywają narzędzia do wyjaśniania decyzji systemów SI, również tych opartych na sieciach neuronowych. Przykładem takiego narzędzia jest SHAP, które wykorzystuje teorię gier do oceny wkładu poszczególnych cech w decyzje modelu. Dzięki takim narzędziom, nawet w przypadku skomplikowanych modeli, można uzyskać wgląd w to, które cechy miały kluczowy wpływ na konkretne decyzje. Niestety, techniczna łatwość wykorzystania tych narzędzi sprawia, że są one nadużywane, a wyjaśnialność uzyskiwana z ich pomocą – nadinterpretowana. W szczególności wartości SHAP nie mogą być wykorzystywane do wnioskowania przyczynowego. Jednak dobre zrozumienie istoty działania narzędzi do wyjaśnialności oraz dostarczanego przez nie wyniku pozwala na zwiększenie transparentności systemu i próbę zrozumienia sposobu podejmowania przez system decyzji. To z kolei jest kluczowe dla użytkowników końcowych, takich jak analitycy bezpieczeństwa, którzy wymagają nie tylko skutecznych prognoz, ale także klarowności w procesie podejmowania decyzji przez sztuczną inteligencję.

W przypadku modułu Malware Hunter AI decyzja systemu może być wyjaśniona przez centralny serwer SI, dostarczając użytkownikowi informacji zwrotnej zawierającej zestaw parametrów aplikacji mobilnej wskazującej na złośliwość aplikacji według modułu. Natomiast moduł Remote Checker stosuje silnik regułowy kojarzący wiele przesłanek wskazujących na użycie zdalnego pulpitu. Końcowa zagregowana ocena jest wynikiem oceny siły i istotności poszczególnych przesłanek. Możliwe jest w każdym przypadku podanie wartości składowych elementów, które złożyły się na konkretną ocenę.

2. Wiarygodność SI a legislacja

Szybki rozwój sztucznej inteligencji i zastosowanie jej w kolejnych obszarach wpłynął na działania legislacyjne mające uregulować wykorzystanie systemów SI. W Stanach Zjednoczonych prezydenckie rozporządzenie wykonawcze ds. bezpiecznej i wiarygodnej sztucznej inteligencji[1] ma na celu podjęcie działań przez odpowiednie agencje rządowe w trybie natychmiastowym.

Tymczasem Unia Europejska jest w trakcie ostatniej fazy przygotowania tzw. „AI Act" mającego na celu ustanowienie jednolitych zasad i norm dotyczących korzystania z technologii sztucznej inteligencji w UE. W rozporządzeniu tym prawdopodobnie zostanie zdefiniowana grupa systemów SI tzw. wysokiego ryzyka. Co istotne, to czy system SI będzie sklasyfikowany jako system wysokiego ryzyka, będzie zależało od tego, w jaki sposób i w jakim celu zostanie zastosowany. Do obszarów wysokiego ryzyka zaliczono m.in. krytyczną infrastrukturę, sądownictwo, a także podstawowe usługi prywatne i publiczne, pod którymi kryją się m.in. usługi bankowe, a jako przykład podawane są systemy oceny zdolności kredytowej. Systemy wysokiego ryzyka, według rozporządzenia, mają podlegać rygorystycznym obowiązkom przedwdrożeniowym, wśród których znajduje się zapewnienie wysokiej wiarygodności systemu. Zatem dobrze mieć na uwadze wiarygodność systemu już od początku jego wytwarzania, a w czasie prac kierować się podejściem *„trustworthy by design"* (wiarygodność z założenia).

Podsumowanie

Badanie wiarygodności systemów SI stanowi wyzwanie i znaczący koszt, jednak wydaje się konieczne w obliczu rosnącego wpływu tych systemów na nasze życie. Należy pamiętać o zyskach przy wprowadzaniu na rynek rozwiązań o wysokiej wiarygodności wynikających z wyższej jakości i transparentności, bezpieczeństwa, zgodności ze zmieniającą się legislacją, a przede wszystkim zwiększonego zaufania do wdrażanego systemu.

Mimo dostępności narzędzi ułatwiających ostateczną ocenę wiarygodności systemów sztucznej inteligencji wysoka wiarygodność powinna być wynikiem staranności całego procesu tworzenia systemu. Kuszące jest stworzenie systemu z pominięciem pewnych aspektów wiarygodności, a następnie sprawdzenie tego aspektu na końcu procesu. Jednak taka praktyka może przynieść zgubne konsekwencje. Dokładna weryfikacja wszystkich elementów składających się na wiarygodność systemu może okazać się niezmiernie trudna i kosztowna. Ponadto, sam techniczny audyt systemu nie rozwiąże wszystkich istotnych pytań, np. czy dane wykorzystane do trenowania zostały pozyskane zgodnie z przepisami prawa.

Dbanie o wiarygodność systemu SI przekłada się nie tylko na zwiększone zaufanie użytkowników i minimalizuje ryzyko błędnego działania, ale również zapewnia zgodność z obowiązującymi i nadchodzącymi regulacjami dotyczącymi m.in. prywatności, bezpieczeństwa oraz transparentności. Dlatego podejście polegające na „wiarygodności z założenia", połączone z cykliczną weryfikacją techniczną systemu, skoncentrowaną na kluczowych kwestiach w danej domenie, wydaje się najbardziej obiecujące. •

1 https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence.

DIGITAL BANKING ACADEMY

Cena (netto)

399 zł

MODUŁ/ os.

~~4389 zł~~

3300 zł

WEŹ UDZIAŁ W ROCZNYM KURSIE

PAKIET 11 SZKOLEŃ

www.digitalbankingacademy.com.pl

Harmonogram 2024

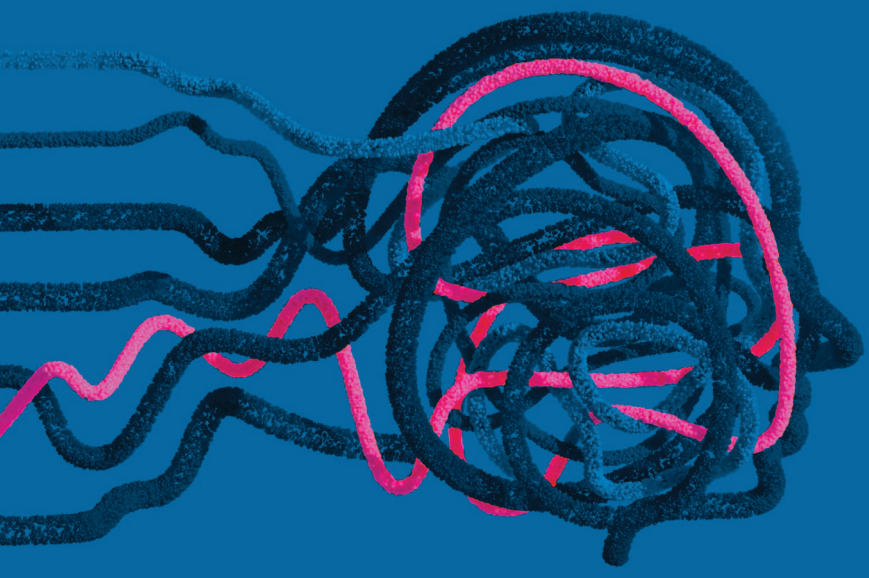
- Legislacyjna roadmapa dla banków na 2024
- ESG dla instytucji finansowych
- LinkedIn dla bankowców
- Transformacja zwinna w praktyce
- Bankowość mobilna i usługi dodane
- Employee Experience w bankowości (dedykowane HR)
- MiCA, blockchain i tokenizacja
- Świadomy konsumeryzm
- Identyfikacja elektroniczna klientów
- Płatności cyfrowe
- Sztuczna inteligencja

Kontakt:
Katarzyna Cechowska-Jastrzębska
k.cechowska@wydawnictwocpb.pl
tel. (22) 623 84 53; tel. kom. 885 885 923

Organizatorzy

ZWIĄZEK BANKÓW POLSKICH

Centrum Procesów Bankowych i Informacji



Szósta edycja interaktywnych warsztatów online z zakresu nowoczesnych rozwiązań cyfrowych

Tematyka
Najbardziej aktualne i przyszłościowe zagadnienia cyfrowe. Szczegółowe, pogłębione i przede wszystkim merytoryczne wystąpienia. Otwarta dyskusja. Czas na zadawanie pytań. Materiały szkoleniowe.

Prelegenci
Wybitni eksperci i praktycy reprezentujący czołowe kancelarie prawne, największe banki, wyróżniających się dostawców technologii, pracowników uczelni, firm doradczych i najbardziej innowacyjne firmy z Polski i świata.

Perspektywy

Każdy temat przewodni omawiany z perspektywy prawnej, regulacyjnej, biznesowej i technologicznej. Dzięki temu w pełni zrozumiesz omawiany obszar, poznając korzyści, wyzwania i ograniczenia z kilku perspektyw.

Czas
Zaoszczędź czas. Dołącz do nas i zdobądź skondesowaną dawkę wiedzy podczas codzinnego, interaktywnego szkolenia online.

Weź udział w szóstej edycji interaktywnych warsztatów online z zakresu nowoczesnych rozwiązań cyfrowych

2019–2023

- **5** edycji
- **56** warsztatów
- **375** godzin wykładów
- **530** ekspertów
- **3920** uczestników

www.digitalbankingacademy.com.pl

DOWIEDZ SIĘ WIĘCEJ

Biometria – najpewniejsza metoda ochrony

Upowszechnienie sztucznej inteligencji jest równoznaczne z przejściem transformacji cyfrowej na całkiem nowy poziom, a z możliwości, jakie daje uczenie maszynowe, doskonale zdają sobie sprawę cyberprzestępcy. To zaś skutkuje potrzebą reorientacji podejścia do zapobiegania fraudom, dokonywanym z użyciem kradzionej tożsamości w kanałach zdalnych. W przypadku usług bazujących na voice recognition eksperci przestrzegają: wystarczy kilkusekundowa próbka głosu dowolnego człowieka, by odwzorować go w sposób znacząco utrudniający wykrycie fałszerstwa przy użyciu tej metody weryfikacji. Naprzeciw oczekiwaniom sektora finansowego wychodzi Platforma Biometrii Behawioralnej BIK, dostarczając nowy wymiar możliwości dokonania weryfikacji tożsamości klienta, który jest niezwykle trudny do podrobienia.

Fot. basiczto/stock.adobe.com

Wyścig zbrojeń pomiędzy twórcami zabezpieczeń a przestępcami do złudzenia przypomina postęp w technice wojennej na przestrzeni wieków. Tak, jak w czasach nowożytnych dynamiczny rozwój artylerii sprawił, że budowa imponujących, warownych zamków straciła rację bytu, podobnie i rozwiązania IT, które zapewniały najwyższy poziom bezpieczeństwa online jeszcze kilka lat temu, dziś okazują się bezradne wobec coraz bardziej wyrafinowanych taktyk, stosowanych przez sprawców. Doskonałym przykładem może być biometria głosowa, do niedawna uchodząca za silny model weryfikacji tożsamości klienta, korzystającego z telefonicznych contact center. W sytuacji, kiedy cybergangi potrzebują tak niewiele, by zacząć „mówić cudzym głosem", ta forma weryfikacji może okazać się niewystarczająca, by stwierdzić, kto jest po drugiej stronie słuchawki.

Socjotechniczne zwodzenie klienta

Podobnie zresztą wszelkie schematy wieloskładnikowego uwierzytelniania podczas logowania się do bankowości elektronicznej lub mobilnej z reguły są bezradne wobec przypadków, kiedy zwiedziony socjotechnicznymi sztuczkami klient sam dopuszcza przestępców do swych zasobów bankowych, np. udostępnia-

jąc im dane uwierzytelniające lub wyrażając zgodę na instalację tzw. zdalnego pulpitu. W takiej sytuacji sam moment logowania nie budzi żadnej wątpliwości, czynności tej dokonuje bowiem upoważniona osoba trzymając się reguł, wyznaczonych przez bank lub innego dostawcę usług finansowych. Przestępca przychodzi później, niejako „na gotowe", kiedy wrota do cyfrowego sejfu są już w pełni otwarte.

Nieprzypadkowo jeden z głównych kierunków aktywności oszustów stanowią właśnie szeroko rozumiane działania socjotechniczne, poczynając od fraudów metodą „na wnuczka" bądź „na policjanta" czy innymi permutacjami tego schematu, aż po rozsyłanie korespondencji z zainfekowanym załącznikiem, którego otwarcie skutkuje przechwyceniem danych do logowania na konto bankowe, lub, co gorsza, instalacją zdalnego pulpitu. Niekiedy zamiast lęku, przestępcy wykorzystują również naszą chciwość, oferując niebotyczne zyski na fikcyjnych platformach, używając często w nazwach tych platform zwrotu ze „sztuczną inteligencją". I choć trudno w to uwierzyć, całkiem sporo ludzi „traci głowę", otrzymując propozycję intratnego zarobku praktycznie bez wysiłku.

Jak podkreśla **Michał Łukasiewicz**, dyrektor Biura Systemów Antyfraudowych BIK i członek zarządu Digital Fingerprints S.A., w samym 2022 r. ponad 106 tys. Amerykanów straciło ponad 6,3 mld dolarów w wyniku oszustw inwestycyjnych[1].

Niska świadomość zagrożeń

Coraz popularniejszym narzędziem, stosowanym przez oszustów jest spoofing, czyli podszywanie się pod numery telefonów, e-maile lub strony www należące do uznanych dostawców usług, także finansowych. Do historii przeszły przypadki, kiedy sprawcy posługiwali się sfałszowanym adresem strony internetowej banku, gdzie litera a w słowie bank była celowo zamieniona na „bnk". Użycie stosowanej m.in. w języku wietnamskim litery w miejscu pierwszej litery polskiego alfabetu skutecznie uchodziło uwadze wielu użytkowników. Można się spodziewać, że wraz z rozwojem narzędzi bazujących na AI pojawią się dziesiątki nowych schematów przestępczej aktywności, których obecnie nawet nie jesteśmy w stanie przewidzieć. Warto podkreślić, że sprawcom nie zawsze chodzi tylko o pieniądze, niekiedy znacznie cenniejszym łupem jest tożsamość ofiary. Dysponując cudzymi danymi osobowymi, sprawcy są w stanie wyłudzić kredyt lub pożyczkę, o czym poszkodowany dowiaduje się najczęściej z chwilą... odwiedzin komornika.

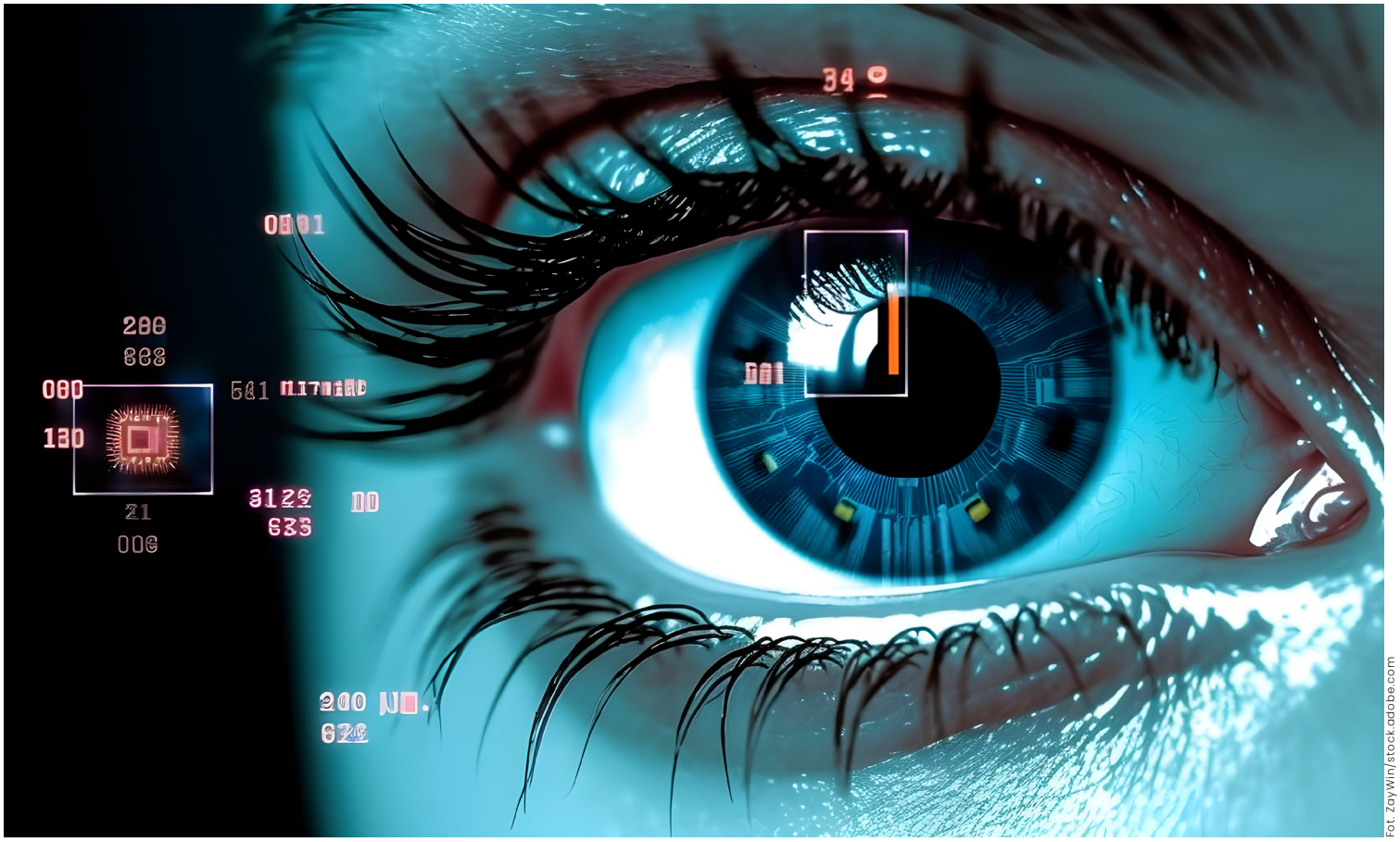
Cichym sprzymierzeńcem zorganizowanych grup przestępczych w tym przynoszącym olbrzymie zyski procederze jest niski poziom świadomości potencjalnych ofiar odnośnie zagrożeń. Analizy BIK za rok 2023 nie pozostawiają wątpliwości: aż 36% naszych rodaków doświadczyło próby wyłudzenia, jednocześnie co dziesiąty z nich nie widzi nic niepokojącego w wycieku danych, a co piąty adresat e-maila nie zadaje sobie nawet trudu, by sprawdzić, czy wiadomość faktycznie pochodzi z zaufanego źródła.

Nieprzemyślane zachowania konsumentów nie są jedynie domeną kanałów elektronicznych; czterech na pięciu naszych rodaków nie poczuwa się do obowiązku, by zastrzec swój dowód osobisty, paszport czy inny dokument w przypadku jego kradzieży lub zagubienia, pomimo iż niemal dwie trzecie z nich ma świadomość, jaki użytek mogą zrobić sprawcy z przechwyconych danych osobowych. Podobnie zresztą pod odbraniu przesyłki z paczkomatu czy od kuriera, co czwarty adresat wyrzuca do śmieci opakowanie, pozostawiając na nim etykietę zawierającą komplet danych osobowych.

Owa bezrefleksyjność, bo w takich przypadkach nie sposób mówić jedynie o nieświadomości, przynosi łatwe do przewidzenia konsekwencje: co piata próba oszukańcza pozwala sprawcom osiągnąć cel. A przecież wskazane sytuacje stanowią niejako abecadło bezpiecznego funkcjonowania w gospodarce elektronicznej. Trudno zatem spodziewać się, by konsumenci byli w stanie skutecznie stawiać czoło zaawansowanym taktykom socjotechnicznym, w rodzaju spoofingu bądź vishingu, skoro tak często ignorują znane od lat reguły postępowania. I nie jest to tylko domeną klientów indywidualnych, również i profesjonalni uczestnicy obrotu gospodarczego, od których należałoby wymagać znacznie większej świadomości, nierzadko zachowują się jak przysłowiowe dzieci we mgle.

Przedsiębiorcy równie niefrasobliwi

Dość przytoczyć najświeższe analizy BIK, z których wynika, iż jedynie kilkanaście procent przedstawicieli sektora MŚP instaluje na swych urządzeniach jakiekolwiek narzędzia antyfraudowe. Jeśli wziąć pod uwagę, iż w tym samym czasie 18% firm doświadczyło próby oszukańczej, łatwo dojść do wniosku, że dla sporej części small biznesu dopiero utrata środków w wyniku fraudu mogłaby stanowić czynnik, skłaniający do zainteresowania się bezpieczeństwem swych środków w kanałach cyfrowych. Można tu przywołać stare przysłowie, zgodnie z którym generałowie są doskonale przygotowani na wojny, które już się odbyły: popularna do niedawna metoda oszustwa na sfingowaną fakturę szybko traci popularność, gdyż pomni złych doświadczeń właściciele firm lub osoby odpowiadające za płatności weryfikują dane zawarte w tych dokumentach (w szczególności numer konta) oraz podstawę do dokonania zapłaty, rzecz w tym, że cybergangi również zdają sobie sprawę, że tą metodą wiele już nie osiągną. Stąd rosnąca liczba maili phishingowych, zawierających rzekome oferty lub wezwania do zapłaty – co jest znacznie groźniejsze, umożliwia →



Fot. ZayWin/stock.adobe.com

bowiem przestępcom przejecie kontroli nad całym rachunkiem firmy. A przecież prowadząc działalność gospodarczą należy zachować maksimum ostrożności, także odnośnie tzw. fraudów wewnętrznych. Również i w tym przypadku AI znacząco sprzyja stosowaniu socjotechniki przez sprawców, zwłaszcza jeśli uświadomimy sobie, że spora część małych firm (a nawet i niektóre średnie) nie stosuje jednolitych procedur w zakresie wewnętrznego przepływu informacji, a telefon od szefa (lub świetnie naśladującego jego głos przestępczego bota) nierzadko uruchamia wysłanie przelewu...

Ustawodawcy chronią beztroskich klientów

Wszystkie te ryzyka dotykają bezpośrednio dostawców usług finansowych, w tym oczywiście banki. Co drugi przedstawiciel bankowości komercyjnej jest zdania, że rok 2023 przyniósł ożywienie kryminalnej aktywności, co nie jest dobrym prognostykiem, jeśli wziąć pod uwagę, iż rok wcześniej co trzeci respondent z tej branży dostrzegał rosnące zagrożenie cyberprzestępczością. Po raz kolejny okazuje się też, że tworzenie zabezpieczeń na własną rękę przez poszczególne podmioty przypomina dziś budowę zamku w epoce rozkwitu artylerii: aż 80% bankowców upatruje największego zagrożenia w atakach socjotechnicznych, a ponad połowa dodaje do tego posługiwanie się cudzą tożsamością przez przestępców. To z kolei oznacza, że jedynym skutecznym sposobem na przeciwstawienie się sprawcom może być wykorzystanie rozwiązań umożliwiających analizę interakcji z klientem na bieżąco i wykrywanie wszelkich odchyleń od normy jako punktów ewentualnego nadużycia czy wręcz fraudu. Do takiego podejścia skłania nie tylko taktyka stosowana przez cybergangi, ale i prokonsumenckie trendy w tworzeniu regulacji.

Jeszcze do niedawna zapisy polskiej Ustawy o usługach płatniczych, przewidujące konieczność zwrotu środków w terminie D+1 klientowi, który uznał dokonaną z jego rachunku operację płatniczą za nieautoryzowaną, słusznie traktowano za omyłkę w implementacji dyrektywy PSD2, która mówiła jedynie o właściwym uwierzytelnieniu osoby, inicjującej płatność. Zaprezentowany niedawno projekt rozporządzenia PSR, które w wielu obszarach ma zastąpić PSD2, nie pozostawia wątpliwości, iż unijny ustawodawca zamierza przyjąć za wzór przepisy obowiązujące w Polsce.

Niezależnie od ostatecznego rezultatu prac nad wspomnianymi regulacjami, należy liczyć się z sukcesywnym przesuwaniem odpowiedzialności z konsumenta na instytucje finansowe, jako profesjonalnych uczestników obrotu gospodarczego. Tymczasem gra idzie o całkiem pokaźne sumy – co dziesiąta spośród instytucji finansowych, ankietowanych przez BIK, poniosła straty z tytułu cyberfraudów przekraczające 10 mln zł w skali rocznej.

Najwyższy poziom zabezpieczenia banku i klienta

Dziś najskuteczniejszym sposobem, by – uwzględniając niesprzyjające uwarunkowania, w tym w szczególności nieświadomość czy wręcz dezynwolturę konsumentów, ale i konsekwentnie prokonsumenckie trendy regulacyjne – ograniczyć przestępczą aktywność wydaje się analiza behawioralna. Współczesne algorytmy uczenia maszynowego umożliwiają wykreowanie unikalnego profilu interakcji danego użytkownika z komputerem, tabletem bądź smartfonem. – *Dzięki zaawansowanym mechanizmom uczenia maszynowego system – np. na podstawie tempa wciskania klawiszy na klawiaturze czy ruchów myszą – jest w stanie ocenić, czy na rachunek loguje się uprawniona osoba, a w razie zagrożenia – zablokować transakcję* – zapewnia **Bartosz Wójcicki**, Product Owner Platformy Biometrii Behawioralnej BIK.

Mechanizm analizy behawioralnej został wykorzystany jako podstawa funkcjonowania **Platformy Biometrii Behawioralnej BIK**. To rozwiązanie pionierskie nie tylko na rynku polskim, ale i w skali europejskiej, umożliwia bowiem weryfikację interakcji użytkownika ze swym urządzeniem z jednoczesnym zachowaniem bezkontekstowości, co zapewnia poszanowanie prywatności i pełną zgodność ze standardami w zakresie ochrony danych osobowych, w tym w szczególności RODO oraz wymogów określonych w przepisach dotyczących usług płatniczych. Weryfikacja przebiega podczas całego trwania sesji, co wyklucza możliwość niewychwycenia przypadku, kiedy zmanipulowanego użytkownika konta zastępują przestępcy, po uprzedniej instalacji tzw. zdalnego pulpitu.

Rozwiązanie jest przy tym komfortowe zarówno dla banku, jak i jego klientów. Ci ostatni zyskują dodatkową, wymierną ochronę przed utratą pieniędzy czy przejęciem dostępu do konta nie tylko całkowicie nieodpłatnie, ale też bez konieczności instalowania jakichkolwiek dodatkowych aplikacji w swym urządzeniu czy też wprowadzania loginów, haseł bądź tokenów. Przeciętny Kowalski nawet nie poczuje, że jego kontakty z bankiem zostały objęte nowym, najwyższym dostępnym na rynku poziomem zabezpieczenia.

Z kolei w przypadku banków kluczowym benefitem, związanym z posługiwaniem się Platformą Biometrii Behawioralnej BIK jest sektorowy charakter całego przedsięwzięcia. Poszczególne modele użytkowników są udostępniane wszystkim uczestnikom Platformy w ramach współpracy sektorowej banków, co zwiększa poziom ochrony klientów, a w konsekwencji również samych banków przed ewentualnymi roszczeniami poszkodowanych przez przestępców użytkowników kont czy ewentualnymi szkodami reputacyjnymi. Warto podkreślić, że sektorowa usługa BIK wykazuje dalece posuniętą elastyczność technologiczną, a umiejscowienie jej właśnie w BIK stwarza możliwości jej dalszego rozwoju, również poza sektorem bankowym. W dobie, kiedy zakres usług, świadczonych przez poszczególnych dostawców, przenika się coraz silniej, a ekosystem sprzedażowe i crosselling zyskują na znaczeniu, zyskuje to szczególny wymiar.

– *Podstawą wszystkich sektorowych rozwiązań BIK jest współpraca. To jeden z ważniejszych czynników sukcesu zaawansowanych rozwiązań oferowanych przez BIK związanych z bezpieczeństwem. Dobrym dotychczasowym przykładem sektorowego rozwiązania z zakresu bezpieczeństwa jest Platforma Antyfraudowa BIK, która zatrzymała już oszukańcze wnioski kredytowe na kwotę ponad 700 mln zł, oznaczając je jako próby wyłudzenia. To potwierdza, że wymiana informacji pomiędzy zainteresowanymi instytucjami przynosi wymierne korzyści dla całego sektora finansowego i jego klientów* – mówi **Agnieszka Szopa-Maziukiewicz**, dyrektor Zarządzająca Obszarem IT w BIK i prezes zarządu Digital Fingerprints S.A., należącej do Grupy BIK.

– *Kolejnym sektorowym rozwiązaniem zapobiegającym fraudom jest Platforma Biometrii Behawioralnej BIK. Chroni klienta i jego transakcje w kanałach elektronicznych. W przypadku biometrii współpraca nabiera szczególnej wagi, ponieważ oznacza szybsze budowanie profili zasilanych z wielu banków jednocześnie. Stwarza to równocześnie możliwość użycia już zbudowanych profili przez każdego z uczestników platformy, co w praktyce oznacza lepszą ochronę wszystkich klientów* – dodaje prezes zarządu Digital Fingerprints S.A.

Aktualnie kilka banków wdrożyło rozwiązanie BIK oparte na biometrii behawioralnej do ochrony swoich klientów. Kilka innych banków jest na etapie procesów podłączania się do rozwiązania Platformy Biometrii Behawioralnej BIK, budując wspólny system bezpieczeństwa w polskim sektorze bankowym. Bazując na dobrych doświadczeniach z działania Platformy, BIK planuje wyjść ze swoim rozwiązaniem na rynki zagraniczne. Aktywnie współpracuje w ramach ACCIS, międzynarodowego stowarzyszenia zrzeszającego m.in. największe biura kredytowe na świecie i przez relacje z nimi stara się rozpowszechnić to rozwiązanie.

[1] https://www.comparitech.com/blog/information-security/investment-scams/

Cyberbezpieczeństwo w erze chmury, sztucznej inteligencji i szalonego tempa wdrożeń

Migracja aplikacji firm sektora finansowego do chmury trwa w najlepsze. Biznes niemal natychmiast odczuwa ulgę po stronie kosztowej i intensywniej skupia się na swojej kluczowej działalności, dzieląc się odpowiedzialnością za swoje IT z dostawcami usług chmurowych. Ten słuszny pęd zmniejsza czujność, jaką branża finansowa, w szczególności podmioty nadzorowane, powinny zachować w odniesieniu do cyberbezpieczeństwa i wdrażanych rozwiązań security – przekonują eksperci GFT.

Fot. greenbutterfly/stock.adobe.com

Bezpieczna chmura

Kiedy dzielimy współodpowiedzialność z dostawcą usług chmurowych, który sam zapewnia nas o podążaniu za najwyższymi standardami bezpieczeństwa i zgodności regulacyjnej, możemy ulec złudnemu poczuciu, że chmura niejako sama zadba o ochronę przed cyberatakami. Tymczasem ta odpowiedzialność jest współdzielona i nie zwalnia firm z samodzielnego budowania wielowarstwowej architektury bezpieczeństwa (defense in depth). Wiara w to, że serwisy chmurowe oferują bezpieczeństwo „by design" jest myśleniem życzeniowym, choć dostawcy realizują swoje obowiązki na najwyższym, światowym poziomie.

Trendy wykładniczego wzrostu ilości cyberzagrożeń na świecie oraz setki tysięcy nowych typów złośliwego oprogramowania dziennie, odzierają nas ze złudzeń – to musi być walka na wspólnym froncie dostawców chmurowych i klientów. A istnienie zabezpieczeń w serwisach chmurowych nie oznacza, że są one skonfigurowane adekwatnie do potrzeb firmy, lub że w ogóle te mechanizmy są domyślnie uruchomione.

Dane są obecnie najcenniejszą walutą i ich ochrona, rozumienie, i interpretacja w kontekście specyfiki danej firmy, jest tak samo ważne, jak analiza zagrożeń dokonywana przez dostawcę chmury.

Dodatkowo ilość informacji wejściowych związanych ze stanem bezpieczeństwa firmy oraz danych wyjściowych do analizy i wnioskowania na ich podstawie – jest przytłaczająca.

– *Co roku najwięksi dostawcy chmurowi dzielą się statystykami z prób nieautoryzowanego dostępu do kont osób prywatnych i firm. Prób takiego logowania do aplikacji w serwisach chmurowych Microsoftu, zidentyfikowanych przez AAD Identity Protection (usługa zabezpieczająca przed nieautoryzowanym dostępem) było dwa lata temu prawie sześć miliardów, więc w tym roku ta liczba z dużą pewnością przekroczy kilkanaście miliardów. Ta cyfra wprawia w osłupienie, a przecież mówimy tutaj tylko o próbach logowania na konta i to konta jednego z wielu dostawców chmurowych* – podkreśla **Przemysław Kulesza, head of Global Security Practice, GFT**.

Wyścig zbrojeń

Automatyzacja detekcji błędnych konfiguracji bezpieczeństwa oraz automatyzacja wykrywania zagrożeń i podejmowania decyzji bez udziału człowieka w celu ochrony przed cyberzagrożeniami, stają się koniecznością, zwłaszcza, że czas analizy i reakcji działa na korzyść wyłącznie cyberprzestępców. Analiza heurystyczna i behawioralna, a także bazy wiedzy o śladach działalności złośliwego oprogramowania (IoC, Indicator of Compromise) i wektorach ataków są już od kilku lat standardem. W tym czasie dostawcy rozwiązań bezpieczeństwa muszą już myśleć o włączaniu dużego modelu językowego (LLM, Large Language Model) w kluczowe procesy detekcji zagrożeń i podejmowania decyzji. Trudno nazwać to jedynie tymczasową modą, kiedy przestępcy angażują sztuczną inteligencję (SI) i LLM do wzmocnienia swojego przestępczego oręża, począwszy od generowania zaawansowanych kampanii phishingowych, przez podszywanie się pod wysoko postawione osoby (tzw. whailing attacks), a skończywszy na skalowaniu nowych technik ataków, w tym APT i DDoS (tzw. AI-Assisted Attacks).

– *Automatyzacja rozwiązań bezpieczeństwa w oparciu o ML jest już z nami od dłuższego czasu, jednak to, co oferują obecne modele AI/LLM można dla zobrazowania nazwać „rozpoznawaniem wzorców na sterydach". Mówimy tu nie tylko o szybkim wykrywaniu znanych problemów czy schematów działania przestępców, ale o wykrywaniu schematów, o których ludzkość jeszcze nie zdążyła pomyśleć. AI to oczywiście miecz obosieczny, ponieważ z jednej strony pozwoli nam skuteczniej odpowiadać na najbardziej złożone ataki, katalogować je (jak np. rozróżnianie grup APT), z drugiej zaś strony da przestępcom możliwość praktycznie nieograniczonej nauki zachowań ludzi i naszych systemów ochrony, doprowadzając do problemu ciągłego wyścigu zbrojeń. Wbudowanie w rozwiązania bezpieczeństwa AI/LLM jest więc koniecznością, nawet przy wszystkich swoich słabościach związanych choćby z wciąż dużą liczbą halucynacji w odpowiedziach tych modeli* – wyjaśnia **ekspert i architekt bezpieczeństwa GFT, Adrian Dąbrowski**.

Autodetekcja zagrożeń i błędnie skonfigurowanych aplikacji w chmurze, a także autonomiczne odpowiedzi na nie, czyli autoremediacja, będą więc coraz mocniej ujawniać się w funkcjonalnościach produktów security.

Kompleksowe podejście na trudne czasy

Zespół cyberbezpieczeństwa GFT przeprowadził dogłębny, trwający prawie półtora roku test (PoC, Proof-of-Concept) rozwiązań klasy Cloud-Native Application Protection Platform (CNAPP), podsumowując ich mocne i słabe strony. Rozwiązania te są dedykowane dla wdrożeń chmurowych i posiadają zazwyczaj architekturę wielowarstwową, umożliwiającą detekcję błędnych konfiguracji bezpieczeństwa (Cloud Security Posture Management – CSPM), a także wykrywanie ataków na aplikacje, maszyny wirtualne i kontenery (Cloud Workload Protection Platform – CWPP). Mogą one też ostrzegać o nadmiarowych lub zbyt wysokich uprawnieniach użytkowników chmurowych (Cloud Infrastructure Entitlement Management – CIEM). Warto zauważyć, iż część z nich już od dawna bazowała na ML, długo przed boomem związanym z ChatGPT i LLM. Co również ważne, rozwiązania CNAPP posiadają moduły compliance, analizujące bieżący stan bezpieczeństwa IT środowisk chmurowych firmy względem światowych standardów uznawanych przez branżę, np. CIS Benchmarks. To pozwala zachowywać zgodność z wymogami przepisów prawa i rekomendacjami nadzoru KNF.

– *Biorąc pod uwagę tempo wzrostu cyberataków w Polsce i na świecie, uważam rozwiązania CNAPP za „must have", nawet z ich niedoskonałościami czy błędami wieku dziecięcego. W czasie testu PoC zastanawialiśmy się z zespołem czy detekcja np. 90% błędnych konfiguracji względem wymagań CIS Benchmark dla różnych rozwiązań chmurowych, to dobry, czy jednak nieakceptowalny, wynik. Zwróćmy uwagę, że w tych 10% niewykrytych luk może czaić się potencjalnie prosta i niebezpieczna furtka wtargnięcia do systemów firmy, ujawniająca także niedopuszczalną niezgodność z wymogami regulatora. Konkluzją było powołanie specjalizacji w zespole cyberbezpieczeństwa GFT, kształcącej osoby definiujące brakujące polisy dla tych przykładowych 10% niewykrytych błędnych konfiguracji. Z jednej strony to nisza usługowa, którą jak wierzymy nasi klienci docenią za jej indywidualizm, z drugiej zaś – wiemy już obecnie, że potrzebują oni wsparcia eksperckiego, ponieważ sami mają istotne ubytki kadrowe na stanowiskach związanych z bezpieczeństwem. Poza tym większość błędów bezpieczeństwa we wdrożeniach chmurowych to właśnie deficyty kompetencyjne czy po prostu brak* →

Fot. Manaj/stock.adobe.com

możliwości dbania o bezpieczeństwo w świecie cotygodniowych wdrożeń zmian na produkcję – wyjaśnia Przemysław Kulesza.

Według różnych raportów dostawców rozwiązań bezpieczeństwa dla chmury, błędne konfiguracje usług stanowią ponad 60% wszystkich problemów z bezpieczeństwem wdrożeń chmurowych. Wśród głównych przyczyn wymienia się braki kompetencyjne, błędy ludzkie, braki punktów kontrolnych bezpieczeństwa w procesie wytwarzania oprogramowania oraz wysokie tempo wdrażania zmian na środowiska produkcyjne, nie pozwalające zespołom wdrożeniowym na jakościowe rewizje i audyty bezpieczeństwa.

Ufaj, ale sprawdzaj

Zespół GFT Polska podchodzi do bezpieczeństwa w chmurze holistycznie, rozumiejąc indywidualne wymagania klientów i różne apetyty na ryzyko. Dlatego CNAPP może być wdrażany w podejściu czysto prewencyjnym, bez uruchamiania autoremediacji, których firmy czasem obawiają się w bardziej skomplikowanych scenariuszach czy krytycznych biznesowo aplikacjach. W takich przypadkach oferowanym rozwiązaniem jest modernizacja części remediacyjnej architektury bezpieczeństwa IT, czyli SIEM/SOAR, które są dedykowanymi rozwiązaniami detekcji i obsługi incydentów. Rynek SIEM/SOAR w Polsce posiada wysokie nasycenie, co wynika z regulacyjnej konieczności ich wdrażania, szczególnie w sektorze finansowym. Klienci jednak ciągle borykają się z problemami ich wydajności, priorytetyzacją alertów, czy po prostu z wysoką ceną tej klasy rozwiązań. Stąd obszar ten wymaga modernizacji:

– Wdrożenie automatyzacji dla obsługi incydentów bezpieczeństwa jest koniecznością w obecnych czasach, żeby skutecznie reagować na wykryte zagrożenia. Wielu specjalistów myśli o wdrażaniu rozwiązań XDR (Extended Detection and Response), jako antidotum. Ale dopiero połączenie takich metod z nowoczesnymi rozwiązaniami SIEM/SOAR daje możliwość kompleksowego pokrycia i skutecznej korelacji zdarzeń w środowiskach multi- czy hybrid-cloud. Innym wyzwaniem

do zaadresowania jest ilość logów koniecznych do analizy przez SIEM/SOAR, która rośnie w zabójczym tempie. Ich analizowanie, korelowanie i składowanie to ciągłe wyzwanie, na które nie ma jednej prostej odpowiedzi. Ciągle balansujemy na cienkiej krawędzi zastanawiając się, które logi możemy składować wyłącznie dla celów potencjalnej analizy wstecznej, a które musimy mieć dostępne i przeszukiwalne online w czasie niemal rzeczywistym. Racjonalne podejście pozwala zachować odpowiednią skuteczność przy utrzymaniu niezbędnej ilości zbieranych logów do spełnienia wymagań regulacyjnych, jak również wymagań zespołu Centrum Operacji Bezpieczeństwa (SOC, Security Operations Center). Wykorzystanie nowoczesnych rozwiązań cloud-native SIEM/SOAR dobrze adresuje te wyzwania. Jako GFT wybraliśmy dla naszej firmy rozwiązanie Microsoft Sentinel, a pamiętajmy, że mamy ponad 10 tys. pracowników rozproszonych po całym świecie. W związku z tym spodziewamy się poziomu 25 MB logów przypadających na każdego z nich dziennie – to potężna ilość rocznie. Obecnie też sami oferujemy produkt Microsoft Sentinel naszym klientom, również jako uzupełnienie rozwiązań XDR, widząc ogromny potencjał modernizacyjny w podejściu SIEM/SOAR amerykańskiej firmy. Zwracam uwagę szczególnie na część SOAR, która pozwala automatyzować reakcje na alerty, pozostawiając zespołom SOC do manualnej analizy wyłącznie najbardziej zaawansowane przypadki – wyjaśnia **Marek Dwórznik, cloud security architect w GFT**.

Fot. KanawatTH/stock.adobe.com

Sektor finansowy w Polsce zwraca uwagę na rozwiązania Microsoftu także z bardziej generalnej przyczyny, mianowicie z powodu niedawnego otwarcia centrum przetwarzania danych Azure w Polsce (Azure Poland Central) w trzech niezależnych lokalizacjach niedaleko Warszawy. Restrykcyjne regulacje czy rekomendacje nadzoru KNF można będzie spełnić szybciej i z mniejszym ryzykiem braku zgodności. GFT od lat wspiera polski i światowy sektor bankowy w konfiguracji usług chmurowych w Azure, ale także Google Cloud i AWS.

– Nasze metody zabezpieczania usług chmurowych i landing zones cechuje podejście indywidualne i ukierunkowane na potrzebę klienta oraz kontekst jego działania. Jednocześnie dbamy o to, aby nasze rekomendacje i wdrożenia bazowały na wymogach przepisów prawnych, światowych standardach bezpieczeństwa (jak ISO 27001, CIS Benchmark) i rekomendacjach nadzoru (w Polsce przede wszystkim mówimy o tzw. Komunikacie chmurowym UKNF ze stycznia 2020 r.). Nie skupiamy się wyłącznie na aspektach technicznych lub regulacyjnych, za to wspólnie tworzymy implementacje bezpieczne i wspierające klienta, realizujące wartość biznesową. W uzasadnionych przypadkach potrafimy też powiedzieć twarde „nie" chmurze, np. przy szyfrowaniu danych bez użycia kluczy zarządzanych przez bank czy przy zbyt niskiej kontroli uprawnień. Stawiamy na jasny i otwarty dialog oraz solidną, uczciwą ekspertyzę – wyjaśnia **Bartłomiej Skowronek, lead architect w GFT**.

Sektor finansowy w Polsce podchodzi ostrożnie, a czasem nieufnie do rozwiązań chmurowych – szczególnie, gdy mówimy o przetwarzaniu danych stanowiących tajemnicę bankową czy przy innego rodzaju danych chronionych. Ostrożność i chłodna kalkulacja są cenne, dlatego GFT chętnie i systematycznie uczestniczy w wyjaśnianiu jasnych i ciemnych stron wdrożeń i migracji do chmury, buduje zaufanie przy użyciu najlepszych dostępnych narzędzi, sprawdzonego podejścia i przejrzystej komunikacji. Jako certyfikowany partner największych dostawców chmurowych na świecie, GFT dostarcza ekspertyzę i bezpieczne wdrożenia chmurowe szyte na miarę, a jednocześnie czerpiące ze swoich doświadczeń globalnych. •

Czy backup Twojego banku na pewno jest adekwatny do zagrożeń?

Kopia zapasowa jest obecnie podstawowym sposobem zabezpieczenia firmowych danych. Nie zawsze jednak wystarcza, aby zagwarantować należyty poziom ochrony oraz wysoką dostępność jednego z najcenniejszych zasobów każdej organizacji.

Artur Matzka
DYREKTOR CENTRUM KOMPETENCJI IT INFRASTRUCTURE, CLOUD, EUC
INTEGRATED SOLUTIONS

Rozwiązania umożliwiające sprawne odzyskiwanie danych w sytuacji problemowej są fundamentalnym elementem firmowego środowiska IT. Pozwalają uchronić organizację przed skutkami awarii sprzętu, usterek aplikacji, błędów ludzkich, a także klęsk żywiołowych.

Klasyczny backup nie w pełni chroni jednak przed efektami wszystkich zdarzeń, które mogą negatywnie wpłynąć na bezpieczeństwo, dostępność, bądź użyteczność firmowych danych. Szczególne znaczenie mają tu działania cyberprzestępców, niezależnie od kierujących nimi pobudek.

Lepiej zapobiegać niż leczyć

Praktyka pokazuje, że firmowe systemy zapewniające ciągłość dostępu do danych muszą nadążać za zmieniającymi się zagrożeniami. Szczególnym przykładem są tu stale przybierające na sile i coraz bardziej złożone ataki zakładające zaszyfrowanie firmowych danych w celu wymuszenia okupu. Jak wynika z analiz firmy Sophos, w roku 2022 przy użyciu ransomware zaatakowane zostało aż 2000 organizacji (66%) na świecie spośród 3000 reprezentujących je uczestników badania. Trzy na cztery (76%) z tych ataków doprowadziły do faktycznego zaszyfrowania danych i przyczyniły się do realnych strat biznesowych[1].

Co ważne, z uzyskanych przez Sophos rezultatów wynika, że zdecydowana większość (97%) organizacji, które padły ofiarą ataku ransomware, ostatecznie była w stanie odzyskać swoje zbiory danych. Przy tym 70% z nich wykorzystało posiadane kopie zapasowe, co potwierdza kluczowe znaczenie tej metody protekcji danych w zapobieganiu dalekosiężnym skutkom takich ataków. Jednocześnie, aż 46% respondentów badania przyznało się do zapłaty okupu. To oznacza, że w przypadku wielu zaatakowanych organizacji odtworzenie z kopii zapasowych nie w całości spełniło oczekiwania i mimo wszystko cyberprzestępcom udało się wzbogacić. Przypuszcza się, że okup zapłaciły organizacje bogatsze, prowadzące rozległe biznesy, które nie mogły sobie pozwolić na przedłużającą się niedostępność danych i zbyt długi proces ich odtworzenia z kopii. Można z tego wnioskować, że nie każdy system backupu okazuje się w pełni użyteczny w kontekście biznesowych wymagań dotyczących czasu odtworzenia.

Zabezpieczenia adekwatne do zagrożeń

Wymuszenia oraz inne długotrwałe ataki oparte na uzyskaniu nieautoryzowanego dostępu do środowiska IT i ukrywaniu tego faktu przez długi czas, generują ryzyka, w przypadku których tradycyjny backup okazuje się niewystarczający. Może się zdarzyć, że kopia zapasowa zostanie utworzona lub zmodyfikowana już w pierwszej fazie ataku, więc jej przywrócenie nie wyeliminuje zagrożenia.

Należy zatem sięgnąć po inteligentne rozwiązania, które z jednej strony chronią dane w sposób gwarantujący ich niezmienność i odporność na ataki, a z drugiej – dają pewność, że dane w kopii zapasowej nie są uszkodzone ani zainfekowane oraz mogą zostać szybko i poprawnie odtworzone.

Właśnie takie technologie oferuje CYFROWY BASTION – architektura referencyjna Integrated Solutions oparta na najlepszych komponentach od globalnych producentów, uzupełnionych sprawdzonymi narzędziami i praktykami bezpieczeństwa adekwatnymi do współczesnych zagrożeń.

Integrated Solutions na straży danych sektora finansów

Integrated Solutions, w roli integratora ICT, przez 12 lat swojego istnienia z powodzeniem zrealizował kilkadziesiąt projektów związanych z budową systemów kopii zapasowej dla klientów z sektora bankowości, ubezpieczeń i administracji publicznej. W roku 2023 zdecydowaliśmy się na skoncentrowanie naszych najlepszych doświadczeń w tej dziedzinie i stworzyliśmy CYFROWY BASTION – referencyjną architekturę systemu kopii zapasowych, doskonale adresującą potrzeby związane z ochroną danych przed skutkami ataków ransomware. Służymy pomocą i możemy zademonstrować w działaniu kompletny system backupu, który jest w stanie ochronić dane, a co najważniejsze, sam dba o to, żeby ich kopie były wiarygodne i bezpieczne. Doświadczenie naszych inżynierów pozwoli zaś zbudować system w taki sposób, aby jego parametry, w tym czas odtwarzania, spełniały indywidualne potrzeby biznesu. Zachęcamy do przetestowania opisywanego powyżej rozwiązania w Państwa środowisku. •

1 „The State of Ransomware 2023", Sophos 2023, https://www.sophos.com/en-us/content/state-of-ransomware

INTEGRATED SOLUTIONS | ARCHITEKTURY REFERENCYJNE

SECURITY

CYFROWY BASTION

To kompleksowe zabezpieczenie firmowych danych oraz pewność ich szybkiego i poprawnego odtworzenia

„Porozmawiajmy o tym, co możemy zrobić dla bezpieczeństwa danych w Twojej organizacji”

Artur Matzka
Dyrektor Centrum Kompetencji
IT Infrastructure/Cloud/EUC
Integrated Solutions

MULTICLOUD CONTAINERS EDUCATION SECURITY WORKSPACE GREEN

ZESKANUJ
I DOWIEDZ SIĘ WIĘCEJ

Wewnątrzsektorowa wymiana informacji i edukacja klientów to najskuteczniejsze działania antyfraudowe

Z WACŁAWEM MAJKĄ, Architektem rozwiązań biznesowych VSoft SA, rozmawiał **Konrad Machowski**.

Fot. VSoft SA

Fraudy kredytowe stanowią jedno z głównych ryzyk, z jakimi na co dzień mierzą się instytucje finansowe. Wraz z dynamicznym rozwojem zdalnych kanałów transakcyjnych rośnie zagrożenie ze strony cyberprzestępców, którzy stosują coraz bardziej zaawansowane i wyrafinowane techniki oszukańcze. Nasuwa się pytanie, które z nich nabierają szczególnego znaczenia dziś, w dobie triumfalnego pochodu sztucznej inteligencji?

– Próby oszukańcze na pewno stanowią olbrzymie wyzwanie dla instytucji finansowych, ale i całej gospodarki. Trudno szacować, jaką skalę przybiera ten proceder, choćby z uwagi na fakt, iż mamy do czynienia z danymi poufnymi, niechętnie ujawnianymi przez banki, jak i organa ścigania, ale również dlatego, że wiele tego rodzaju działań jest dziś udaremnianych na bardzo wstęp-

nym etapie, przez algorytmy stosowane w sektorze finansowym. Z całą pewnością istnieje związek pomiędzy zmianą formuły obsługi klienta a schematami, stosowanymi przez przestępców. **Obecnie coraz więcej procesów odbywa się w kanałach zdalnych, bez bezpośredniego kontaktu pracownika banku z klientem, co było standardem jeszcze kilka lat temu**, przed wybuchem pandemii COVID-19. Dziś znacznie łatwiej uzyskać pozytywną decyzję kredytową, nie trzeba w tym celu dostarczać szeregu dokumentów, a dodatkowo w przypadku zobowiązań na niższe kwoty decyzja taka podejmowana jest nierzadko w sposób automatyczny, czy wręcz z wykorzystaniem systemów uwierzytelniania dostarczanych przez podmioty trzecie. Tak jest chociażby w przypadku zakupów ratalnych za pośrednictwem platform e-commerce, gdzie klient wnioskuje o kredyt z poziomu tej platformy, nierzadko nie mając nawet świadomości który z dostawców usług finansowych współpracujących z danym portalem udzieli mu kredytu. W takich sytuacjach mamy do czynienia z integracją obu partnerów za pośrednictwem interfejsów API, których rozwój znacznie przyspieszył po wprowadzeniu dyrektywy PSD2. Stwarza to całkiem nowe możliwości; w tradycyjnej gospodarce trudno byłoby sobie wyobrazić, żeby klient licytujący rower czy telewizor na platformie aukcyjnej ubiegał się o sfinansowanie zakupu tego przedmiotu wchodząc na odrębną aplikację banku. Dziś jest to możliwe, dzięki czemu sektor finansowy zyskuje nowe źródło przychodów. Należy jednak pamiętać, iż w takich sytuacjach kluczowe jest należyte wypośrodkowanie pomiędzy bezpieczeństwem a wygodą. Zakup przedmiotu za kilkaset złotych powinien być szybki i dokonywany w modelu one click, takie są doświadczenia współczesnych konsumentów. Procedura bezpieczeństwa powinna być zatem tak skonstruowana, by nie tworzyć istotnego wyłomu w tych oczekiwaniach, a zarazem zabezpieczyć dostawcę usług finansowych przed próbami oszukańczymi.

Jaką zatem strategię winny przyjąć banki, by postawić tamę coraz bardziej wyrafinowanym próbom wyłudzenia, zwłaszcza w obliczu rosnącej presji konsumentów na zakupy proste, intuicyjne i „one click"?

– **Zwalczanie fraudów kredytowych w bankach powinno mieć obecnie charakter wieloetapowy**, poczynając od weryfikacji tożsamości użytkownika. Ta z kolei nie obejmuje już wyłącznie samego uwierzytelnienia, ale również analizę zachowania klienta, pod kątem wykrywania ewentualnych anomalii wskazujących na to, że po drugiej stronie mamy do czynienia z kimś innym. Jeśli np. klient, który nigdy nie opuszczał swego miejsca zamieszkania, nagle usiłuje dokonać transakcji z odległego państwa, to już jest pierwszy sygnał, że możemy mieć do czynienia z oszustwem, a podejrzenie to przechodzi w pewność np. z chwilą ustalenia, że od czasu ostatniej transakcji dana osoba fizycznie nie była w stanie przemieścić się tak daleko. Wówczas instytucja finansowa może zastosować pełen wachlarz mechanizmów bezpieczeństwa, poczynając od telefonu do klienta, by się upewnić czy dana operacja jest inicjowana przez niego, a kończąc na zablokowaniu transakcji. Ta ostatnia opcja nie zawsze jest optymalna, trzeba wziąć pod uwagę, iż może ona doprowadzić do uniemożliwienia płatności za całkiem legalną transakcję np. w restauracji czy na stacji paliw, co z kolei frustruje użytkownika i w konsekwencji oddziałuje źle na wizerunek instytucji finansowej.

Bardziej zaawansowaną formułą jest wykorzystanie biometrii, w szczególności analizy behawioralnej. Chodzi o rozpoznanie unikalnego sposobu interakcji użytkownika z urządzeniem: sposobu pisania na klawiaturze, ruchów myszą czy dotykania ekranu w smartfonie. W trakcie obsługi aplikacji czy systemu bankowości elektronicznej ten uczy się owego indywidualnego wzorca, a wszelkie odchylenia od tegoż, zwłaszcza w sytuacjach ryzykownych, jak zaciąganie kredytu czy też dokonywanie płatności na duże kwoty, stanowi bardzo wiarygodną przesłankę, iż mamy do czynienia z próbą oszukańczą. Najważniejszy z punktu widzenia bezpieczeństwa klienta, ale i instytucji finansowej, jest fakt, iż **analiza behawioralna umożliwia również wykrycie usiłowania fraudów dokonywanych z udziałem socjotechniki, kiedy manipulowany przez oszustów użytkownik sam dokonuje przelewu na obce konto czy też wypełnia wniosek kredytowy**. Badania naukowe wykazały, iż w takich przypadkach człowiek zachowuje się inaczej aniżeli gdyby decyzje te podejmował samodzielnie – i ową rozbieżność jesteśmy w stanie zidentyfikować posługując się technikami behawioralnymi. Jak widać, beneficjentem nowoczesnych technologii są nie tylko oszuści, dają one również legalnie działającym podmiotom możliwość zapewnienia ochrony na poziomie dotychczas niewyobrażalnym.

To szczególnie istotna konstatacja, tym bardziej jeśli weźmiemy pod uwagę, iż szkody spowodowane fraudami czy wyciekiem danych nie są jedynie natury finansowej, równie dobrze instytucja może być ukarana przez nadzorcę lub doznać uszczerbku reputacyjnego...

– Tak, właściwie wszystkie te sytuacje w ostatecznym rozrachunku generują straty finansowe. Kary nakładane przez organy nadzorcze idą w miliony złotych, co stanowi równowartość strat poniesionych w wyniku poważnego →

wyłudzenia. Podobnie i **uszczerbek reputacyjny skutkuje utratą zaufania wśród klientów i bardzo często ich ucieczką**, co oznacza szkody trudne do oszacowania, acz z reguły znacznie wyższe aniżeli nawet samo wyłudzenie kredytu o sporej wartości. O ile w tym ostatnim przypadku mamy do czynienia z jednorazowym, choć bez wątpienia dotkliwym zdarzeniem, przed którym na dodatek dość łatwo się zabezpieczyć korzystając z dobrodziejstw nowoczesnej technologii, to nadszarpnięta reputacja może ciągnąć się za danym podmiotem przez całe lata czy nawet dekady, skutecznie ograniczając dopływ klientów, niekiedy nawet w sposób bezpowrotny. Konsekwencją w niektórych sytuacjach może być nawet upadłość instytucji, zwłaszcza finansowej, które tradycyjnie już są traktowane jako podmioty zaufania publicznego. Dlatego właśnie **tak istotnym zadaniem dla współczesnych instytucji bankowych jest udaremnianie prób oszukańczych dokonywanych na szkodę klientów, nawet jeśli dotyczą one relatywnie niewielkich kwot**. Dla konsumenta decydująca w takich sytuacjach nie jest utrata kilkuset złotych, tylko fakt, że bank, który powinien zapewnić powierzonym przezeń środkom pełne bezpieczeństwo, zawiódł jego zaufanie.

Rzecz w tym, że najlepszym „wspólnikiem" cyberoszustów jest nierzadko ich ofiara. Jakże wielu użytkowników bankowości elektronicznej lub mobilnej podchodzi do kwestii bezpieczeństwa z lekceważeniem, uważając że to bank powinien zapewnić ochronę ich pieniędzy. Czy zatem w ogóle możemy mówić o skutecznej ochronie zasobów klienta, jeśli on sam nie czuje się w obowiązku zachować należytej ostrożności? Zwłaszcza w sytuacji, kiedy regulatorzy sprzyjają takiemu przesuwaniu odpowiedzialności na banki, by wspomnieć choćby niedawno opublikowany projekt unijnego rozporządzenia PSR i zawarte w nim podejście do transakcji nieautoryzowanych...

– W tym obszarze wiele zależy od specyfiki samego konsumenta. Inne błędy popełniać będą seniorzy nieoswojeni z funkcjonowaniem nowoczesnych rozwiązań lub wręcz mający problemy z zapamiętywaniem credentiali, w ich przypadku głównym problemem jest zapisywanie sobie haseł czy loginów, czy to w formie tradycyjnej, jako kartka noszona w portfelu obok karty płatniczej, czy też w aplikacji mobilnej bądź systemie bankowości elektronicznej. Po drugiej stronie będziemy mieli przypadki ewidentnej niefrasobliwości, jak choćby w przypadku osób ulegających próbom oszukańczym w rodzaju tzw. nigeryjskiego szwindlu czy przelewających oszczędności na rzekome inwestycje w kryptowaluty czy rynek FOREX, które okazują się fraudem. Wobec każdej z tych sytuacji trzeba stosować nieco inną miarę. O ile w przypadku seniorów faktycznie należy wziąć pod uwagę ich specyficzne ograniczenia wynikające z wieku, w konsekwencji zaproponować im inną formę uwierzytelniania niewymagającą zapamiętywania skomplikowanych ciągów znaków, w postaci choćby autentykacji biometrycznej w rodzaju face ID czy odcisku palca, to fraudy „inwestycyjne" ograniczyć można jedynie konsekwentną edukacją. Nie jesteśmy w stanie inaczej oddziaływać na użytkownika, który nie dość że świadomie i dobrowolnie przelewa środki na konto wskazane przez oszustów, to jeszcze czyni to w błogim przekonaniu, że trafił na inwestycję życia.

Zawsze **na pierwszym miejscu będzie uświadamianie, zwłaszcza w obliczu pojawiania się coraz to nowszych schematów oszustw, z których wielu użytkowników kanałów zdalnych nawet nie zdaje sobie sprawy**. Wezwanie do zapłaty zaległego rachunku za media, informacja o zajęciu komorniczym, gdzie wystarczy kliknąć w link do rzekomej spłaty zadłużenia, by zostać przekierowanym do strony prowadzonej przez oszustów, czy choćby popularne, zwłaszcza w okresie przedświątecznym, SMS-y z prośbą o dopłatę za zamówioną przesyłkę czy opłacenie cła – w każdym z tych przypadków mamy do czynienia z przestępcami, którzy chcą przejąć nasze środki czy też zaciągnąć kredyt wykorzystując nasze dane osobowe. Stąd tyle ostrzeżeń, żeby nie klikać w podejrzane linki, gdyż grozi to instalacją na naszym urządzeniu tzw. zdalnego pulpitu, przez który złodzieje mogą mieć stały dostęp do naszych zasobów.

Oczywiście trzeba wymagać od ludzi ostrożności, jednak równocześnie trzeba im uświadamiać, jakie zachowania mogą być podejrzane. Nie w każdym przypadku niewłaściwe zachowanie będzie przejawem dezynwoltury czy niefrasobliwości. Jeśli ktoś faktycznie czeka na zagraniczną przesyłkę i dostaje informację od rzekomej agencji celnej, by uregulować wszystkie opłaty, to jeśli nie będzie świadom, że takie wiadomości wysyłają oszuści, z pewnością da się złapać. Podobnie w przypadku sfingowanych stron banków, które od oryginału odróżnia jedna literówka czy użycie znaku niespotykanego w polskim alfabecie, acz łudząco podobnego do tego, który znajduje się w adresie banku. Równolegle należy oczywiście stosować mechanizmy antyfraudowe, w tym analizę behawioralną, jednak nie powinno być to realizowane kosztem edukacji. Gospodarka elektroniczna ma to do siebie, że wymaga wyrobienia w sobie określonych zachowań, żeby czuć się bezpiecznie. Jeśli nie będziemy edukować konsumentów, to mimo stosowania wymyślnych systemów zabezpieczeń zagrożenie zawsze będzie rosnąć.

Banki od dawna wymieniają się informacjami o zagrożeniach, czy w obliczu nowych ryzyk, związanych z digitalizacją rynku, proces ten zapewnia nowe możliwości w zakresie prewencji?

– **Wewnątrzsektorowa wymiana informacji ma kluczowe znaczenie dla zminimalizowania poziomu zagrożenia fraudami**. Jeśli dana instytucja zidentyfikuje źródło zagrożenia, czy to w postaci przestępczej lokalizacji czy unikalnego sposobu posługiwania się urządzeniem przez oszusta, a następnie przekaże to do podmiotu zajmującego się wymianą danych o zagrożeniach, znacząco ułatwia działania antyfraudowe innym bankom. Nie muszą one za każdym razem przeprowadzać skomplikowanej analizy, wystarczy że na początku odfiltrują działania podejmowane ze skompromitowanych adresów lub przez podejrzane osoby. Takie rozwiązania działają też prewencyjnie wobec samych sprawców, jeśli będą oni mieli świadomość, iż wiedza o zidentyfikowanych próbach oszukańczych jest dostępna dla wszystkich podmiotów w sektorze, wówczas będą mniej skłonni do wykorzystywania tych samych zasobów do kolejnych wyłudzeń. Nie trzeba chyba dodawać, iż wydatnie utrudnia to życie przestępcom, z korzyścią dla banków oraz ich klientów. Wówczas nawet instytucja dysponująca słabszymi narzędziami antyfraudowymi jest chroniona na najwyższym poziomie.

Skuteczność platform antyfraudowych jest tym większa, im więcej podmiotów się z nimi integruje i przekazuje im dane, nie tylko o fraudach, ale również np. o obsłudze kredytu przez poszczególnych użytkowników. Na podstawie zgromadzonych danych możemy wychwycić symptomy, że dana osoba za jakiś czas może mieć problem z obsługą zobowiązania, wówczas bank jest w stanie reagować odpowiednio wcześniej, choćby poprzez zaproponowanie konsolidacji, wakacji kredytowych czy innego mechanizmu wsparcia, by nie dopuścić do sytuacji, kiedy dane zobowiązanie przestanie być obsługiwane. Jesteśmy oczywiście w stanie również zidentyfikować przypadki, kiedy dany klient zaczyna zachowywać się niestandardowo, np. bombardując poszczególne podmioty wnioskami kredytowymi. To może być zarówno przejawem próby oszukańczej, ale równocześnie zwiastować sytuację, kiedy dana osoba popadła w tarapaty finansowe i wykonuje nieprzemyślane ruchy, by pozyskać środki na dalsze funkcjonowanie czy prowadzenie biznesu. Tu z pomocą przychodzą raporty kredytowe, które są w stanie wskazać wszystkie działania podejmowane w danym okresie przez konkretną osobę we wszystkich instytucjach wymieniających się danymi za pośrednictwem takiej platformy. Na tej samej zasadzie można wychwycić drobne błędy, które zdarzają się przestępcom podejmującym próby oszukańcze. Ot, choćby takie jak złożenie w różnych instytucjach finansowych sfałszowanych zaświadczeń o zatrudnieniu tego samego klienta, gdzie każde z nich dotyczyć będzie innego miejsca pracy. Istnieje stare porzekadło, że nie ma zbrodni doskonałej, sprawcy z reguły popełniają jakiś drobny, niekiedy niemal niezauważalny błąd, a wymiana informacji i wykorzystanie innowacyjnych narzędzi dostępnych na tego typu platformach zwiększa szansę wychwycenia anomalii.

W tym kontekście chciałbym postawić pytanie o konektory, które są w ofercie VSoft. Na czym polega to rozwiązanie, i w jakim stopniu jego użycie może zwiększyć skuteczność działań antyfraudowych w banku, czy wręcz zwiększyć skuteczność wykrywania prób oszukańczych w całym sektorze? Wreszcie – czy stosowanie konektorów może dać odczuwalną poprawę jakości obsługi również i dla konsumenta?

– Nasza firma ma w ofercie cały zestaw konektorów do różnych instytucji. Ich użycie przede wszystkim upraszcza sam proces wdrożenia. Pamiętajmy, że dostęp do danych z instytucji zewnętrznych nie jest łatwy, szczególnie w branży bankowej, gdzie całe zasoby są mocno odseparowane od świata zewnętrznego z uwagi na zagrożenie wyłudzeniem i kradzieżą danych. **Konektory pomagają zintegrować ową tkankę bankową z danymi, pochodzącymi z zewnętrznych źródeł, także platform antyfraudowych. Dokonywanie wymiany danych z wykorzystaniem konektora zwiększa wydatnie szybkość tego procesu, co znowu przekłada się na realny poziom bezpieczeństwa, nie tylko danej instytucji, ale wszystkich użytkowników danego rozwiązania do wymiany informacji.** Przypomnę po raz kolejny, że sprawcy również grają na czas, zatem szybsze przekazanie informacji o zagrożeniu do innych instytucji może powstrzymać kolejne próby oszukańcze. **Konektory pozwalają też zautomatyzować procesy weryfikacji danych – poprzez dostępne interfejsy API możemy w automatyczny sposób wysyłać zapytanie o informacje i otrzymywać rezultat tą samą drogą**. To z kolei ma szczególne znaczenie w przypadku wspomnianych już produktów masowych, jak kredyty ratalne czy karty, gdzie z uwagi na doświadczenie użytkownika cały proces weryfikacji musi przebiegać jak najszybciej i w trybie całodobowym. Tak jak trudno sobie wyobrazić ręczne procedowanie wniosku o udzielenie rat na skuter wart kilka tysięcy złotych, podobnie nie sposób zakładać, by klient miał cierpliwość oczekiwać kilkanaście czy kilkadziesiąt minut na przekierowanie wniosku do BIK w modelu tradycyjnym. To musi być góra kilkanaście sekund, a posługując się konektorem jesteśmy w stanie osiągnąć ten rezultat. Pod tym względem **konektory pozwalają osiągnąć nie tylko wyższy poziom bezpieczeństwa, ale i poprawić jakość obsługi klienta, co na obecnym rynku, gdzie banki konkurują ze zwinnymi fintechami, ma znaczenie szczególne.** •

Cyfrowa twierdza

Centrum Procesów Bankowych i Informacji
cpb.pl

Grudzień 2023