O świadomości cyberzagrożeń - raport antyfraudowy BIK

W 2023 roku niechlubne czołowe miejsca popularności najczęstszych metod hackerskich zajęły vishing i phishing. Największym problemem w zapewnieniu bezpieczeństwa osób prywatnych i przedsiębiorców jest nadal niska świadomość zagrożeń zarówno wśród osób prywatnych, jak i firm. Pozostawia do życzenia poziom wykorzystania narzędzi na rzecz podnoszenia cyberbezpieczeństwa. To wyraźny sygnał, jaki płynie z Raportu Antyfraudowego BIK 2023, który prezentuje wyniki badań zrealizowanych w trzech segmentach: rynku klientów indywidualnych, małych i średnich przedsiębiorstw oraz banków i korporacji. Badanie pokazało np., że ponad 80% przedsiębiorców nie korzysta z żadnych usług i narzędzi chroniących przed wyłudzeniami. W związku z tym mogą paść ofiarą manipulacji, która pociągnie za sobą straty finansowe.

O ile jednym z najczęstszych działań oszustów w 2022 r. było „fałszowanie dokumentacji finansowej przez klientów wnioskujących o kredyt lub pożyczkę", tak w 2023 r. wśród najczęściej wymienianych oszustw dominowało podszywanie się pod instytucję publiczną w rozmowie telefonicznej. Ataki typu vishing i phinsing zajmują bowiem niechlubne czołowe miejsca wśród najpopularniejszych działań socjotechnicznych ubiegłego roku. Potwierdzają to sami klienci, jak również banki i instytucje finansowe.

Z kolejnej edycji Raportu Antyfraudowego BIK wynika, że przestępcy coraz częściej odchodzą od prób zaawansowanych ataków hakerskich na profesjonalnie chronione systemy IT instytucji finansowych. Koncentrują się zaś na socjotechnice jako dużo skuteczniejszej metodzie, wspieranej nowoczesnymi technologiami. Nie zmienia się za to cel oszustów - zawsze chodzi o nakłonienie ofiary do wykonania czynności, które umożliwiają kradzież.

Ataki socjotechniczne rozwijają się w dynamicznym tempie i przybierają nowe formy. Wzrost skali przestępstw z wykorzystaniem socjotechnik, potwierdza fakt częstszego osobistego kontaktu z co najmniej jedną z takich metod wyłudzeń aż 36 proc. badanych. To więcej o 4 pkt. proc. w stosunku do 2022 r. Pomimo ogólnej świadomości zagrożeń, warto podkreślić, że jest to jednak nadal najsłabsze ogniwo z punktu widzenia bezpieczeństwa osób prywatnych, przedsiębiorców i dużych instytucji finansowych.

Największym wyzwaniem również dla banków są działania z wykorzystaniem socjotechnik stosowanych na ich klientach. Ataki te mają na celu przejęcie dostępów do rachunków, a w rezultacie kradzież środków. Z tego typu zagrożeniem zetknęło się 70 proc. respondentów sektora bankowego. Wyłudzenia, np. kredytów, na skradzione dane osobowe zwróciły uwagę 64 proc. badanych. Dość powiedzieć, że 40 proc. korporacji odnotowuje ponad 500 zdarzeń fraudowych rocznie.

- *Instytucje finansowe, w tym banki, mają bardzo trudne zadanie, by na każdym kroku przypominać swoim klientom, że emocje i pośpiech to podstawowe czynniki, które decydują o skuteczności ataków socjotechnicznych. Konsekwentnie prowadzą działania edukacyjne na temat zmian nawyków w obszarze ochrony przed wyłudzeniem. Oszuści jednak stale doskonalą swoje metody zmieniając taktyki i sposoby ataków. Wydaje się więc, że poza edukacją skuteczną bronią w walce z wszelkimi rodzajami oszustw i wyłudzeń będzie powszechne wykorzystanie nowoczesnych rozwiązań i narzędzi technologicznych, w tym służących do weryfikacji behawioralnej użytkowników bankowości elektronicznej* - mówi Michał Łukasiewicz, dyrektor Usług Antyfraudowych w BIK i członek Zarządu Digital Fingerprints.

Na celowniku oszustów znajdują się także małe i średnie przedsiębiorstwa. Raport BIK dowiódł, że z problemem oszustw w 2023 r. zmierzyło się 60 proc. firm. Co trzecia firma, w wyniku pojedynczego oszustwa, straciła 100 tys. zł. i więcej.

Aż 82,4 proc. przedsiębiorstw nie korzysta z usług lub narzędzi antyfraudowych. Ich odsetek jeszcze wzrósł od 2022 r. o 2,6 pkt. proc. W sektorze MŚP dominuje bowiem jeszcze przeświadczenie, że wystarczy zdrowy rozsądek, by zapobiegać wyłudzeniom. To złudne przekonanie, tym bardziej, że gros przedsiębiorstw jest w posiadaniu danych swoich klientów i pracowników, którym należy zapewnić odpowiednie metody ochrony. W przeciwnym razie, w wyniku np. wycieku danych klientów może to narazić podmiot na ryzyko pozwów i na wysokie kary administracyjne. W przypadku małych firm, wysokość kar może przesądzić nawet o tym, że znikną z rynku.

***

Raport Antyfraudowy BIK 2023, to druga edycja cyklicznej publikacji , w której poddano analizie trzy segmenty rynku: klientów indywidualnych, małe i średnie przedsiębiorstwa oraz banki i korporacje. Badanie trwało kilka miesięcy, koncentrując uwagę zarówno na obszarze ochrony danych, jak również na tematyce poziomu bezpieczeństwa osób i biznesu. W Raporcie Antyfraudowym zostały wykorzystane wyniki badań opinii zrealizowanych na zlecenie BIK przez instytut badawczy Quality Watch (Cyberbezpieczeństwo Polaków), Instytut Keralla Research (Zdarzenia fraudowe i cyberataki na firmy MŚP w Polsce) oraz własne badanie ankietowe wśród przedstawicieli dużych firm z rynku (Zdarzenia fraudowe w korporacjach). W Raporcie znajdują się nie tylko analizy i dane z badań, ale także merytoryczne komentarze ekspertek i ekspertów BIK oraz ekspertów z organizacji partnerskich: CERT Orange Polska, NASK i CSIRT KNF.

Wszystkich zainteresowanych kompleksowym materiałem nt. zjawiska fraudów w Polsce w 2023 r. oraz wiedzą, jak skutecznie bronić się przed oszustwami w przypadku różnych schematów wyłudzeń, zachęcamy do pobrania bezpłatnego raportu: https://rozwiazania-antyfraudowe.bik.pl/raporty/2023

***

Biuro Informacji Kredytowej jest inicjatorem programu edukacyjnego Nowoczesne Zarządzanie Biznesem i partnerem w module „Zarządzanie ryzykiem finansowym w biznesie i życiu osobistym”

Więcej: www.nzb.pl oraz www.facebook.com/NowoczesneZarzadzanieBiznesem