Równi – pod kątem zagrożeń, ale i zabezpieczeń

Dziś żaden bank nie powinien polegać na zabezpieczaniu tożsamości pracowników za pomocą tradycyjnego hasła. Według raportu Verizon's 2022 Data Breach Investigations Report, prawie 50% naruszeń bezpieczeństwa wiąże się właśnie z wykorzystaniem skradzionych danych uwierzytelniających. Na tym problemie powinny skoncentrować się też banki spółdzielcze, które coraz częściej stają się celem cyberprzestępców. Wielu z nich podczas ataków phishingowych podszywa się pod ich klientów, wykorzystując m.in. fakt, że spółdzielcy doskonale ich znają i oferują im szybkie załatwienie pożyczek czy kredytów.

Ponad 80% incydentów cyberbezpieczeństwa zaczyna się od przejęcia konta użytkownika. Firmy i organizacje – w tym również banki – właśnie w ten sposób najczęściej tracą ważne dane. Banki spółdzielcze stosują dziś technologiczne i proceduralne środki zabezpieczeń przed cyberprzestępcami, w czym pomaga im m.in. Centrum Rozwoju Usług Zrzeszeniowych (CRUZ). Mimo to muszą liczyć się z tym, że intruzi coraz bardziej będą interesować się ich placówkami. Te – zlokalizowane poza głównymi miastami – stają się coraz częściej celem mniej zaawansowanych przestępców, którzy działając z terenów Europy Wschodniej lub Chin, są również trudniejsi w schwytaniu przez policję.

– *Wśród przedstawicieli bankowości spółdzielczej częste jest przekonanie, że wyłudzenia w obszarze transakcji, kredytów czy aplikacji webowych dotyczą głównie banków komercyjnych* – mówi **Krzysztof Góźdź**, dyrektor sprzedaży w Secfense. – *Argumentem na poparcie tej tezy jest zwykle stwierdzenie, iż spółdzielcy znają doskonale swoich klientów i ich zachowania, dlatego trudno im „nabrać się" na podstęp cyberprzestępcy podszywającego się pod osobę im znaną. To może być jednak złudne poczucie bezpieczeństwa. Banki spółdzielcze, podobnie jak komercyjne, oferują swe usługi w internecie, rośnie też odsetek klientów spoza bezpośredniego obszaru ich działania.*

EDUKACJA I TECHNOLOGIA

Myślenie, że lokalne instytucje finansowe są poza zainteresowaniem cyberprzestępców, nie znajduje odzwierciedlenia w rzeczywistości. W obliczu nowych zjawisk, takich jak masowa migracja klientów do kanałów zdalnych czy praca online, lokalne instytucje finansowe stają się takim samym celem intruzów jak banki komercyjne.

Centrum Rozwoju Usług Zrzeszeniowych zajmuje się dostarczaniem sprawdzonych oraz wystandaryzowanych usług, rozwiązań i sprzętu dla banków spółdzielczych. Prowadzi też projekty edukacyjne – również te związane z bezpieczeństwem pracowników banków w sieci.

– *Zdajemy sobie sprawę, że pod kątem stopnia zagrożenia ze strony cyberprzestępców nie różnimy się już aktualnie niczym od największych instytucji finansowych. Dlatego bankowość spółdzielcza również aktywnie włącza się w ochronę swoich klientów, tak indywidualnych, jak i instytucjonalnych* – podkreśla **Paweł Gula** z Centrum Rozwoju Usług Zrzeszeniowych. – *Chcemy przede wszystkim postawić na ochronę tożsamości pracowników, którzy najczęściej stają się celem ataków phishingowych. Inwestujemy więc nie tylko w edukację, ale również w nowe, rodzime rozwiązania technologiczne, które ułatwiają implementację wieloskładnikowego uwierzytelniania.*

GLOBALNY PROBLEM

W Polsce, jak podaje raport ZBP InfoDok, tylko w I kw.br. oszuści podjęli 1915 prób kradzieży z wykorzystaniem przejętych danych osobowych, w sumie na kwotę 575 tys. zł. To średnio aż 21 wyłudzeń dziennie.

Celem ataków bardzo często są banki i instytucje finansowe, które broniąc się przed nimi, wykorzystują różne technologie. Jedną z nich jest MFA, czyli wieloskładnikowe uwierzytelnianie. W bankach – zarówno w Polsce, jak i na całym świecie – technologia 2FA lub MFA nie jest dla nikogo nowością. Globalnym wyzwaniem trzeciej dekady dwudziestego pierwszego wieku pozostaje jednak wysoki poziom skomplikowania i różnorodności środowisk IT oraz implementacja w nich skutecznych metod MFA. Między innymi z tego powodu większość banków stosuje uwierzytelnianie, które nie jest ani wygodne w użyciu, ani wystarczająco odporne na ataki cyberprzestępców.

Według badania firmy HYPR Report: State of Authentication in the Finance Industry 2022, 32% pracowników banków z USA (200 osób), Wielkiej Brytanii (100 osób), Francji (100 osób) i Niemiec (100 osób) nadal korzysta z tradycyjnych metod MFA, takich jak SMS-y i hasła jednorazowe, 43% polega na menedżerach haseł, a 22% wyłącznie na nazwach użytkowników i hasłach.

Fot. Secfense

Krzysztof Góźdź, dyrektor sprzedaży w Secfense.

Fot. CRUZ

Paweł Gula, Prezes Zarządu, Centrum Rozwoju Usług Zrzeszeniowych.

– Kilka lat temu uwierzytelnianie wieloskładnikowe było de facto zaleceniem cyberbezpieczeństwa dla firm i banków. Dziś jednak wyrafinowani intruzi znaleźli sposoby, aby obejść i te zabezpieczenia – wyjaśnia Krzysztof Góźdź z Secfense. *– Aktualnie jedynym rozwiązaniem, w pełni odpornym na phishing oraz kradzież loginów i haseł, jest otwarty i darmowy standard FIDO2, który pozwala na wykorzystanie kluczy kryptograficznych, ale również urządzeń, które zawsze mamy przy sobie, takich jak laptopy z wbudowaną kamerą, Windows Hello lub smartfony z czytnikiem linii papilarnych.*

NIEWYKORZYSTANE I DARMOWE BEZPIECZEŃSTWO

Zdanie specjalistów od bezpieczeństwa IT potwierdzają również osoby na co dzień pracujące w zbadanych przez HYPR instytucjach finansowych. Aż 99% ankietowanych przyznało, że metody uwierzytelniania stosowane w ich organizacjach wymagają unowocześnienia. Nie jest ono jednak aktualnie możliwe, bo stoją mu na przeszkodzie m.in. problemy z integracją (27%) czy zarządzaniem tym procesem (75%).

– Największy kłopot wciąż sprawia implementacja. Wdrożenie MFA jest trudne, uciążliwe i kosztowne. Co więcej, jeśli bank posiada w swojej infrastrukturze IT setki aplikacji – a tak jest przecież w bankach spółdzielczych – masowa implementacja na wszystkich programach jest praktycznie niewykonalna. Efekt? Jedna z najlepszych metod uwierzytelniania, czyli standard FIDO2 – choć zaprojektowany w kwietniu 2018 r. – po ponad czterech latach wciąż jest jeszcze dodatkiem, a nie uniwersalnym sposobem zabezpieczania tożsamości w internecie – mówi Krzysztof Góźdź.

Z podobnym wyzwaniem jeszcze niedawno mierzył się BNP Paribas Bank Polska. Wdrożenie w tej organizacji silnego uwierzytelniania – co istotne bez ingerencji w kod chronionej aplikacji – na masową skalę stało się możliwe dzięki Secfense User Access Security Broker. Dziś bank może stosować silne dwuskładnikowe uwierzytelnianie na poziomie aplikacji i tym samym zabezpieczać całą organizację przed wyłudzaniem informacji i kradzieżą danych uwierzytelniających.

SPÓŁDZIELCZE Z HOLISTYCZNYM MFA

Śladem największych instytucji finansowych idą banki spółdzielcze. Centrum Rozwoju Usług Zrzeszeniowych (CRUZ) podjęło ważną i strategiczną decyzję. Wprowadziło do oferty technologię Secfense, która pomoże w zapewnieniu bankom spółdzielczym takiego samego poziomu bezpieczeństwa dostępu do swoich wewnętrznych aplikacji i danych, jakie mają największe instytucje finansowe w Polsce i na świecie.

– Cieszymy się, że będziemy w stanie zaoferować innowacje, która da bankom spółdzielczym realną możliwość poprawy poziomu zabezpieczenia tożsamości pracowników i użytkowników systemów wewnętrznych i aplikacji – dodaje Paweł Gula. *– Secfense User Access Security Broker to wygodna, łatwa w implementacji – bo nieingerująca w kody – technologia, sprawdzona w największych i najbardziej wymagających bankach.*

Do tej pory implementacja technologicznych nowości w organizacjach o złożonej strukturze IT była droga, złożona, czasochłonna, a czasem nawet niemożliwa. Często banki, firmy czy instytucje nie były w stanie sprostać temu wyzwaniu.

Dzięki rozwiązaniom działającym w warunkach „zerowej" wiedzy o aplikacjach i środowisku informatycznym, umiejącym się uczyć i rozumieć procesy możliwe są szybkie, łatwe i nieingerujące w kod wdrożenia.

To również niezwykle istotne w przypadku banków spółdzielczych, które w dobie coraz szybciej rosnących zagrożeń muszą adaptować swoje środowiska IT i polityki bezpieczeństwa do nowej rzeczywistości. Dobrze, że do wartości, które na co dzień wyznają, czyli solidarności, samopomocy, elastyczności, bliskości, zaufaniu, współzarządzaniu, walce z wykluczeniem finansowym i dbałości o środowisko, dołącza teraz także bezpieczeństwo IT. •