Nic nie jest takie, jakim się wydaje

Michał Jurek
Dyrektor Departamentu Monitorowania Ryzyka i Restrukturyzacji IPS-SGB

Gdy dowiedziałem się, że tematem przewodnim tego wydania „Banku Spółdzielczego” będzie bezpieczne korzystanie z usług bankowości mobilnej i internetowej, popadłem w pewne zakłopotanie. Wszak w jednym z ostatnich felietonów poruszyłem już problematykę socjotechniki i sposobów oddziaływania na ludzi, wykorzystywanych przez przestępców. Pomyślałem jednak, że trafia się dobra okazja, by ten temat jeszcze pogłębić i zwrócić uwagę na wątki, których nie poruszyłem poprzednio.

Tematyka ta jest szczególnie istotna

zważywszy, że to właśnie tzw. cyberzagrożenia stanowią jedno z najpoważniejszych źródeł ryzyka w bankowości, a ich znaczenie nieustannie rośnie. Potwierdza to m.in. badanie prowadzone cyklicznie przez EY oraz Instytut Finansów Międzynarodowych.

Z wypowiedzi przedstawicieli Ministerstwa Cyfryzacji wynika, że Polska jest obecnie jednym z trzech najczęściej atakowanych cybernetycznie państw na świecie.

W edycji ankiety z 2022 r., którą skierowano do zarządzających ryzykiem z 88 banków z 30 krajów, to właśnie cyberzagrożenia uznano za najważniejszy rodzaj ryzyka w działalności bankowej (wskazało tak 72% badanych) w perspektywie kolejnych dwunastu miesięcy. Dopiero na drugim miejscu znalazło się ryzyko kredytowe (59% wskazań). W badaniu przeprowadzonym rok wcześniej kolejność była jeszcze odwrotna.

Co spowodowało koncentrację uwagi zarządzających ryzykiem na cyberzagrożeniach? Przede wszystkim jest to konsekwencją wojny Rosji z Ukrainą, jednym z elementów której stała się wzmożona aktywność grup hakerskich zza naszej wschodniej granicy. Po wybuchu wojny drastycznie zwiększyła się ich aktywność mierzona atakami cybernetycznymi na banki i inne instytucje finansowe. W Polsce, jako kraju frontowym, jest to szczególnie odczuwalne. Z wypowiedzi przedstawicieli Ministerstwa Cyfryzacji wynika, że Polska jest obecnie jednym z trzech najczęściej atakowanych cybernetycznie państw na świecie. Jeszcze w 2022 r. w Polsce zidentyfikowano 30 tys. incydentów dotyczących cyberbezpieczeństwa, podczas gdy w roku 2023 było ich już 80 tys.

Świadomość niesie adekwatne działania

Na szczęście, świadomość niesie ze sobą adekwatne działania. Polskie banki są dobrze zabezpieczone i odporne na cyberzagrożenia. Dostrzegają to również

Niektórzy klienci uważają, że jedno hasło jest niczym tolkienowski Jedyny Pierścień i w zupełności wystarcza, by zarządzać wszystkimi usługami bankowymi, społecznościowymi i innymi.

ich klienci. Wskazują na to wyniki badania „Postawy Polaków wobec cyberbezpieczeństwa”, przygotowywanego pod egidą Związku Banków Polskich na zlecenie Warszawskiego

Instytutu Bankowości, w ramach projektu Bezpieczeństwo w Cyberprzestrzeni. Zgodnie z ubiegłoroczną edycją tego badania, prawie połowa ankietowanych Polaków kolejny rok z rzędu właśnie banki uznała za liderów cyberbezpieczeństwa. Sektor bankowy pozostawił w pobitym polu zarówno wojsko i policję, jak i administrację publiczną. Co więcej, aż 85% ankietowanych stwierdziło, że czuje się bezpiecznie korzystając z bankowości elektronicznej, pomimo występujących cyberataków. To wielki kapitał zaufania.

Niestety, z tak wielką mocą wiąże się wielka odpowiedzialność. Dlaczego – niestety? Otóż dlatego, że większość ankietowanych w przytoczonym powyżej badaniu uważa, że zapewnienie cyberbezpieczeństwa jest zadaniem samych banków (70% wskazań). Jedynie niespełna ¼ badanych zgodziła się z twierdzeniem, że również odpowiada za bezpieczeństwo finansowych usług elektronicznych. Warto też zaznaczyć, że odsetek podzielających ten pogląd systematycznie spada: jeszcze w 2021 r. odpowiedziało tak 29% badanych, podczas gdy w 2023 r. – tylko 24%.

Dlatego tak ważna jest czujność,
a wręcz nieufność do nadsyłanych maili,
domagających się podania danych
osobistych, czy dziwnych rozmów
telefonicznych, których inicjatorzy
mają dokładnie taki sam cel.

Jedno hasło jest niczym tolkienowski Jedyny Pierścień

Nie dziwi więc, że klienci banków, zabezpieczając swoje środki finansowe, idą często po linii najmniejszego oporu. Uważają, że jedno hasło jest niczym tolkienowski Jedyny Pierścień i w zupełności wystarcza, by zarządzać wszystkimi usługami bankowymi, społecznościowymi i innymi. A gdy do tego doda się dbałość o ochronę tegoż hasła i innych danych identyfikacyjnych, bezpieczeństwo jest już pełne.

To bardzo optymistyczne postrzeganie otaczającego nas świata. Czy szanowni Czytelnicy pamiętają jeszcze film Christophera Nolana z 2010 r., o wdzięcznym tytule „Incepcja”? Jego główny bohater zajmował się wykradaniem sekretów z umysłów ofiar w trakcie snu. W ostatnim zleconym zadaniu, będącym osią fabularną filmu, cel jest jednak odwrotny. Chodzi o zaszczepienie w umyśle spadkobiercy ogromnej fortuny pewnego pomysłu (mniejsza o to, jakiego – nie psujmy przyjemności oglądania tym, którzy filmu nie widzieli). W taki też sposób działają dziś hakerzy: ich celem jest przekonanie nas, że czytamy maila wysłanego przez instytucję finansową, odbieramy telefon od pracownika tej instytucji, logujemy się na prawdziwej stronie internetowej naszego banku. Tymczasem w świecie, w którym sztuczna inteligencja została zaprzęgnięta do manipulacji mediami poprzez technikę deepfake, coraz trudniej odróżnić rzeczywistą jawę od hakerskiego omamu.

Dlatego tak ważna jest czujność, a wręcz nieufność

do nadsyłanych maili, domagających się podania danych osobistych, czy dziwnych rozmów telefonicznych, których inicjatorzy mają dokładnie taki sam cel. W tym celu pomocna może być stosowana, analogicznie do ruchu drogowego, zasada ograniczonego zaufania, sprowadzająca się do sentencji, która dała tytuł niniejszemu felietonowi. Warto dopuścić do siebie myśl, że – jak pisał Edgar Allan Poe – „wszystko to, co widzę, wiem – snem jest tylko, we śnie snem”. ●