„CZYNNIK LUDZKI” TO WCIĄŻ NAJSŁABSZE OGNIWO W CYBERBEZPIECZEŃSTWIE. JAK NIE ULEC SOCJOTECHNIKOM ZŁODZIEI DANYCH OSOBOWYCH

W II kwartale br. odnotowano ponad 1800 prób wyłudzeń na łączną kwotę 598 tys. zł – podaje najnowszy Raport o dokumentach infoDOK. Jednak skala nie raportowanych ataków oszustów jest wielokrotnie większa. Mnożą się metody działania złodziei danych, którzy oprócz narzędzi technologicznych, stosują różne formy manipulacji i socjotechniki, by przechwycić dane osobowe.

ALEKSANDRA STANKIEWICZ-BILLEWICZ
Biuro Informacji Kredytowej

Niebezpieczeństwo związane z kradzieżą danych osobowych dotyczy każdego, a skala oszustw z wykorzystaniem cudzej tożsamości nie maleje.

Aż 20 razy dziennie każdy z nas jest potencjalnie narażony na wyłudzenie. W ostatnim kwartale odnotowano 1800 prób wyłudzeń, z których trzy przekroczyły milion złotych - największa miała miejsce w województwie lubuskim i opiewała na 1,35 mln zł. – podaje raport infoDok.

Nie wszystkie próby wyłudzeń kredytów udaje się wychwycić. W zdecydowanej większości dotyczy to kredytów zaciąganych bez intencji zwrotu pożyczonych środków, czyli tzw. fraudów bankowych. Wyniki analiz BIK wskazują, że takich przypadków jest rocznie na kwotę ok. 600 mln zł.

SCHEMATY DZIAŁANIA PRZESTĘPCÓW

Przestępcy modyfikują sprawdzone sposoby wyłudzania danych, wykorzystują ludzką naiwność, brak spostrzegawczości, podatność na socjotechniki. Łączą te podstępne metody wraz z potencjałem nowych technologii, co pozwala uwiarygodnić te działania w odbiorze ich ofiar.

Do bardzo popularnych ostatnio metod socjotechnicznych należą, m.in. spoofing – metoda telefoniczna lub mailowa, polegająca na podszywaniu się pod prawdziwe organizacje (w tym banki), phishing – np. z wykorzystaniem sms lub połączenia telefonicznego.

To sposoby, które bazują na ludzkiej naiwności lub nieuwadze, przenoszą ofiarę na fałszywą, ale łudząco podobną stronę naszej siłowni, ulubionej restauracji czy firmy kurierskiej. Ataki spamowe – rozsyłane linki reklamowe, w które pochopnie klikamy, wszystkie te formy kontaktu mogą wykorzystywać dane pochodzące z wycieku.

Celem wszystkich działań złodziei jest uzyskanie korzyści finansowych - zdobycie dostępu do pieniędzy na rachunku oraz danych osobowych. Najgorsze, że przestępcy działają lawinowo: kiedy już zdobędą czyjeś dane, potrafią w ciągu jednego dnia zaciągnąć na tę osobę nawet kilkadziesiąt pożyczek.

Dane osobowe i kontaktowe w rękach złodziei oznaczają wysokie niebezpieczeństwo. Mogą one zostać wykorzystane przez przestępców do oszustw, wspomaganych poprzez przebiegłe chwyty socjotechniczne.

WYŁUDZENIE „NA TELEFON”

Eksperci BIK obserwują aktywność telefoniczną oszustów podszywających się pod rozmaite instytucje zaufania publicznego i znane firmy w celu zebrania danych personalnych.

Złodzieje, aby przechwycić dane osobowe i wykorzystać je do wyłudzeń kredytów, pożyczek czy abonamentów telefonicznych, stosują metody socjotechniczne. Należy do nich metoda telefoniczna, polegająca na podszywaniu się pod prawdziwe organizacje (w tym

Przestępcy działają lawinowo: kiedy już zdobędą czyjeś dane, potrafią w ciągu jednego dnia zaciągnąć na tę osobę nawet kilkadziesiąt pożyczek.

DOBRE NAWYKI BEZPIECZEŃSTWA DANYCH – WAŻNE RADY, JAK NIE DAĆ SIĘ OSZUKAĆ

1. **Dokonując płatności przez internet – unikaj** otwartych publicznych sieci wifi, korzystaj ze znanej bezpiecznej sieci,

2. **Nie klikaj w żadne linki z sms-ów** – nawet jeśli na pierwszy rzut oka wydają się znajome,

3. **Nie ufaj ofertom obiecującym możliwość łatwego zarobienia** dużych kwot, wysokich wygranych w konkursach czy otrzymania spadku po nieznanym krewnym – to pułapki;

4. **Nigdy nie kontynuuj podejrzanych rozmów** – jeśli masz obawę co do wiarygodności osoby, która dzwoni – natychmiast rozłącz się. Lepiej samemu zadzwonić na oficjalną infolinię firmy, aby potwierdzić czy faktycznie jej pracownik kontaktował się z Tobą;

5. **Pamiętaj: pracownik BIK, Związku Banków Polskich, Twojego banku NIGDY nie pyta się** o login i hasło do logowania na Twoje konto w banku, nie prosi o pełny numer Twojej karty, jej daty ważności oraz kod CVV2/CVC2, ani nie namawia do zainstalowania aplikacji na Twoim komputerze lub smartfonie;

6. **Nie oddzwaniaj na nieznany numer** – to zły odruch, który grozi przekierowaniem do krajów egzotycznych - za takie połączenie nasz operator komórkowy pobierze podwyższoną opłatę;

7. **Zachowaj umiar w przekazywaniu swoich danych w sieci** – unikajmy pochopnych decyzji, klikania na niesprawdzonych witrynach sklepowych. Przemyślmy czy sposób weryfikacji podczas procedury wynajmu na godziny hulajnogi lub samochodu w formule car sharing, na popularnym portalu streamingowym – nie budzi podejrzeń. Uwiarygodnianie scanem dowodu osobistego lub scanem karty kredytowej, to wysoce prawdopodobne pole do możliwych nadużyć z wykorzystaniem cudzych danych;

8. **Miej włączone Alerty BIK** – to wiadomości sms lub e-mail, które przychodzą w momencie, gdy ktoś próbuje zaciągnąć kredyt lub pożyczkę na nasze dane. Dzięki monitorowaniu zapytań o dane z Rejestru Dłużników BIG InfoMonitor, Alerty BIK powiadomią również w sytuacji, gdy ktoś w naszym imieniu podpisuje umowę, np. z firmą telekomunikacyjną na zakup drogiego telefonu z abonamentem, zawiera umowę z operatorem telekomunikacyjnym, dokonuje zakupów na raty. To sposób, by na stałe chronić się przed wyłudzeniem, bo nigdy nie wiadomo, kiedy i skąd nasze dane zostaną skradzione.

   Taka wiadomość pomoże uratować przed stratami finansowymi. Pozwala na szybką reakcję, która jest kluczowa. W Alercie podana jest data oraz nazwa instytucji, w której składany był wniosek – informacja ta pomoże anulować kredyt czy pożyczkę, których sami nie zaciągnęliśmy.

Nie tylko osoby poszkodowane w wyniku wycieku muszą się mieć na baczności, ale wszyscy powinni pilnie zarządzać informacjami o sobie oraz aktywnie korzystać z narzędzi, które chronią przed wyłudzeniem.

banki czy BIK), w której złodzieje wykorzystują narzędzia umożliwiające wykonanie połączenia telefonicznego z wyświetleniem prawdziwego numeru wiarygodniej instytucji, np. znanego dostawcy usług lub banku.

Oszuści dzwonią do przypadkowych osób, najczęściej ofiar wycieków danych. Złodzieje podczas rozmowy brzmią bardzo profesjonalnie, stosując chwyty socjotechniczne, element zaskoczenia, wykorzystują ludzką naiwność lub nieuwagę. Ofiarą tych sugestywnych manipulacji socjotechnicznych może paść każdy. O tym jak może przebiegać taka rozmowa, tłumaczy Andrzej Karpiński, Szef Bezpieczeństwa Biura Informacji Kredytowej:

– Rozmowy nawiązywane przez złodziei danych mogą trwać długo. Z jednej strony potencjalna ofiara poddawana jest manipulowana przez technologię - przestępcy z wykorzystaniem narzędzi potrafią przełączać rozmowę do innych fałszywych „konsultantów", aby upozorować prawdziwy kontakt np. z bankiem. Z drugiej strony, ofiara narażona jest na sugestywne socjotechniki. Złodziej opisuje sytuację kryzysową, która wymaga działania ze strony rozmówcy, aby uniknął strat. Jest duże ryzyko, że nieuważna osoba będąca pod presją, w trakcie codziennych obowiązków ulegnie tej socjotechnice. Dlatego zwracam uwagę na konieczność zachowania szczególnej ostrożności przez nas wszystkich i stosowanie zasady ograniczonego zaufania. Jeżeli zaskakuje nas telefon z firmy, której nie znamy albo od której nie spodziewamy się kontaktu, lepiej natychmiast przerwać połączenie".

„NA WYCIEK" NIC NIE PORADZISZ

Sposoby nieuprawnionego wykorzystania skradzionych danych mnożą się wraz ze zwiększaniem się ruchu w internecie oraz rosnącą popularnością usług telekomunikacyjnych. Niemal każdego dnia słyszymy o wyciekach danych z różnych instytucji, włamaniach na serwery dużych firm, uczelni, urzędów. Kopalnia wiedzy dla hackerów są media społecznościowe. Maja oni zatem do dyspozycji dane pochodzące z wycieków, ale także dane, które niestety nieświadome niczego ofiary – podają im same.

Choć sam wyciek to jeszcze nie wyłudzenie, jednak istnieje duże prawdopodobieństwo wykorzystywania skradzionych danych w przyszłości, np. do spoofingu, ataków phishingowych i spamowych czy wymuszania haseł.

Doniesienia o wycieku danych powinny dać do myślenia, nie tylko aktywnym kredytobiorcom. Nie tylko osoby poszkodowane w wyniku wycieku muszą się mieć na baczności, ale wszyscy powinni pilnie zarządzać informacjami o sobie oraz aktywnie korzystać z narzędzi, które chronią przed wyłudzeniem. Dlatego, jak zaleca szef bezpieczeństwa BIK:

– Uważajmy, gdzie pozostawiamy swoje dane, rozważnie dokonujmy transakcji płatniczych w sieci, dokładnie sprawdzając adresy portali internetowych. Upewnijmy się, czy oddzwaniamy na znany nam numer, nie odpisujmy anonimowym nadawcom. Niewiedza, może nas dużo kosztować. Nie udostępniajmy wszystkich informacji jako publicznych i chrońmy się przed następstwami wycieków, np. poprzez Alerty BIK.