Cyberdefence 24

aut. Sylwia Gliwa 23.01.2019

PKO BP: „LUDZKI FIREWALL” GWARANTEM BEZPIECZEŃSTWA W BANKOWOŚCI? [WYWIAD]

W czasach, kiedy nowe pokolenie rodzi się ze smartfonem w ręku, a bankowość elektroniczna towarzyszy nam na każdym kroku funkcjonowania w sieci, konieczne są nowe zasady zachowania bezpieczeństwa dla klientów indywidualnych. Czy banki są w stanie nauczyć swojego klienta higieny korzystania z sieci, aby użytkownik ewaluował z najsłabszego na najsilniejsze ogniwo systemu zabezpieczeń? Specjalnie dla CyberDefence24.pl o edukowaniu użytkownika opowiedział Piotr Kalbarczyk, Dyrektor Departamentu Cyberbezpieczeństwa, PKO Banku Polskiego.

Sylwia Gliwa: Najsłabszym ogniwem systemu bezpieczeństwa, wciąż pozostaje człowiek, czyli klient bankowości elektronicznej i mobilnej. Jak pan ocenia poziom wiedzy użytkowników w Polsce?

Piotr Kalbarczyk: Jest pewne określenie, które idealnie oddaje wagę jaką w systemie bezpieczeństwa odgrywa człowiek, to „ludzki firewall”. Gdyby wszyscy użytkownicy mieli wystarczający poziom świadomości to wielu ataków udałoby się uniknąć. Niestety wciąż są osoby, które nie zdają sobie sprawy z zagrożeń, jakie na nich czyhają. Uważają często, że za bezpieczeństwo odpowiedzialny jest ktoś inny, nie oni, a cyberprzestępcy skutecznie to wykorzystują stosując nowe i coraz bardziej wyrafinowane i dopracowane metody socjotechniczne.

Nasz bank od dawna informuje, ostrzega i edukuje klientów w kwestiach dotyczących zagrożeń i bezpieczeństwa w sieci. Publikujemy odpowiednie komunikaty w serwisach transakcyjnych, na stronach internetowych banku w materiałach dla klientów, jak i w mediach społecznościowych. Potwierdzeniem skuteczności tych działań jest obserwowana przez nas rosnąca świadomość klientów - coraz częściej zgłaszają nam swoje wątpliwości, podejrzenia dotyczące phishingu. Klienci informują nas o takich przypadkach bardzo szybko, natychmiast po ich wystąpieniu dzięki czemu „bezpiecznicy” mogą natychmiast zareagować na działania cyberprzestępców.

W jaki sposób cyberprzestępcy najczęściej atakują użytkowników? Jakie są główne techniki przez nich wykorzystywane?

Powszechnym zjawiskiem jest phishing. To oszustwo polegające na podszywaniu się pod inne osoby, firmy czy instytucje po to, aby skłonić użytkownika do konkretnych zachowań np. podania swoich danych, w tym loginu i hasła czy kliknięcia w link, który zainstaluje na naszym sprzęcie złośliwe oprogramowanie. Dlatego użytkownicy powinni być szczególnie wyczuleni na maile i wiadomości jakie otrzymują. Czasem wystarczy kilka czynności, jak chociażby sprawdzenie adresu nadawcy, dokładne przyjrzenie się przesłanemu linkowi lub wnikliwe przeczytanie adresu strony www, na której się znajdujemy, aby wiedzieć, czy mamy do czynienia z oszustwem. Szczególnie niebezpieczne są takie, kiedy przestępcy chcą wyłudzić od nas hasło do konta w banku lub numery karty kredytowej. Podanie tych danych na fałszywej stronie może skutkować utratą dużych ilości pieniędzy z konta.

Innym często spotykanym atakiem phishingowym jest podszywanie się oszustów pod firmy świadczące usługi np. telekomunikacyjne albo kurierskie. Przesyłane do losowo wybranych osób maile informują o konieczności dokonania płatności – pod pretekstem zapłaty za fakturę, przesyłkę itp. Wykorzystując zaufanie odbiorcy wiadomości do znanej powszechnie firmy oraz groźbę konsekwencji wynikających z nieuregulowania opłaty, przestępcy skłaniają daną osobę do otwarcia załącznika. W efekcie nieświadomie instalują na swoim sprzęcie złośliwe oprogramowanie, które może wykradać dane albo śledzić wszystkie czynności, jakie wykonujemy z wpisywaniem loginów i haseł włącznie.

Funkcjonując w sieci w sposób nieostrożny, użytkownicy mogą niejako wspomóc działania przestępców i ułatwić włamanie na konto bankowe czy przejęcie danych. Jakie zachowania klientów najbardziej sprzyjają przestępcom i jak się ich ustrzec?

Można powiedzieć, że w tym przypadku jest jak z myciem zębów, obowiązują pewne zasady tzw. higiena podstawowa bez niej przestępcy mają bardzo ułatwione zadanie. Niezabezpieczony komputer, korzystanie z bankowości elektronicznej z publicznie dostępnych komputerów lub otwartej sieci Wi-Fi, udostępnianie swoich danych logowania innym osobom, klikanie w linki, wiadomości pochodzące z nieznanych źródeł przesyłane na adresy mailowe lub konta mediów społecznościowych, nieczytanie lub niesprawdzanie treści SMS-ów autoryzujących – to sytuacje, których należy się bezwzględnie wystrzegać.

Ostrożne i przemyślane zachowanie użytkowników w sieci jest podstawą zachowania bezpieczeństwa, jednakże jaką rolę odgrywa sprzęt i oprogramowanie? Jaką dostrzegają Państwo korelację pomiędzy użytkowanym sprzętem i oprogramowaniem a bezpieczeństwem użytkowników?

Nawet najlepszy sprzęt i najlepsze oprogramowanie nie dadzą nam gwarancji bezpieczeństwa, jeśli nie będziemy przestrzegać podstawowych zasad bezpieczeństwa. Przede wszystkim należy zadbać o zabezpieczenie sieci i routera. Istotnym jest zainstalowanie oprogramowania antywirusowego, które powinniśmy mieć nie tylko na naszym komputerze stacjonarnym, ale też na smartfonie.

To, co jest niezwykle ważne to pobieranie wszystkich instalowanych programów i aplikacji z zaufanych źródeł. Powinniśmy też dokładnie sprawdzić jakich uprawnień wymaga od nas aplikacja czy program, który instalujemy. Istotne jest, żeby przed pobraniem przeczytać opinie użytkowników, aby w ten sposób uniknąć przykrych konsekwencji. Pamiętajmy również o aktualizowaniu aplikacji, systemu, przeglądarki i oprogramowania antywirusowego.

Jak bezpiecznie korzystać z bankowości elektronicznej i mobilnej – jakie 3 najważniejsze rady mógłby Pan dać klientom banków?

Trudno podać trzy najważniejsze zasady czy rady. Te najbardziej podstawowe to:

- Wszędzie tam, gdzie to możliwe należy stosować silne metody uwierzytelnienia.
- Zawsze należy sprawdzać adres strony logowania, najlepiej wpisywać go ręcznie lub logować ze strony głównej banku.
- Uważać na fałszywe maile, wiadomości w mediach społecznościowych przychodzące od nieznanych osób oraz załączniki. Nie należy wchodzić w linki nieznanego pochodzenia.
- Dbać o regularną zmianę hasła i nie zapisywać danych w przeglądarce
- Chronić dane do logowania – nie przekazywać ich nawet najbliższym osobom.
- Nie logować się do serwisów bankowości elektronicznej z ogólnodostępnych komputerów, nie korzystać z nieznanych i niezabezpieczonych sieci wifi

Niedawno przygotowaliśmy dla klientów specjalną kampanię dotyczącą bezpieczeństwa bankowości

mobilnej. Najważniejsze zasady jakie powinni przestrzegać klienci bankowości mobilnej to:

- Sprawdzać treść SMS-ów przed potwierdzeniem transakcji
- Pobierać aplikacje tylko z oficjalnych źródeł
- Sprawdzać, jakich uprawnień wymaga instalowana aplikacja
- Blokować ekran telefonu
- Nie logować się do serwisów z publicznych sieci Wi-Fi
- Pamiętać o ustawieniu limitów transakcji
- Regularnie aktualizować system i aplikacje
- Dokładnie sprawdzać adresy stron sklepów internetowych

O konieczności edukowania użytkowników mówi się od dawna a w przeszłości prowadzono wiele kampanii. Jak Pan ocenia ich skuteczność? Jakie błędy są popełniane w edukowaniu użytkowników?

Banki w Polsce stosują jedne z najnowocześniejszych zabezpieczeń systemów elektronicznych. Mamy świadomość, że możliwości klientów w obszarze informatycznych technologii zabezpieczających są ograniczone i staramy się ich w tym obszarze wspierać. Z drugiej strony tempo rozwoju narzędzi przestępczych powoduje, że co jakiś czas słyszymy o kolejnych atakach. Większość z nich polega jednak nie na ataku na systemy bankowe, a na sprytnej próbie oszukania klienta. Moim zdaniem efektywność szkoleń związana jest bezpośrednio ze sposobem, w jaki edukujemy klientów. Jest słaba, gdy wykorzystujemy tylko metodę nakazów, czyli koncentrujemy się na tym co należy zrobić. Dużo lepszy efekt można uzyskać dodając element wyjaśnienia, dlaczego należy postępować zgodnie z naszymi zaleceniami.

PKO BP jest jednym z najbardziej innowacyjnych i mobilnych banków działających na rynku polskim. Zapewne prowadzą Państwo działania, aby edukować swoich klientów w zakresie bezpieczeństwa korzystania z bankowości elektronicznej i mobilnej - Czy oraz jakie działania przynoszą wymierny skutek?

Edukowanie klientów w zakresie bezpieczeństwa jest bez wątpienia ważnym elementem działań jakie realizujemy w banku. Prowadzimy kampanie edukacyjne w mediach społecznościowych. Ostatnia miała miejsce w grudniu i dotyczyła bezpieczeństwa bankowości mobilnej. Regularnie publikujemy artykuły na naszym portalu Bankomania, gdzie można przeczytać o najczęściej występujących zagrożeniach i sposobach, jak się przed nimi bronić. Publikujemy stosowne ostrzeżenia w serwisach transakcyjnych, na stronach internetowych oraz w materiałach dla klientów. Przykładem takich działań jest też akcja Cyberstrażnik prowadzona w mediach społecznościowych. Jej celem było uświadomienie jak rzadko Internauci zdają sobie sprawę z tego, jak cenne są ich dane osobowe. Chętnie publikują zdjęcia, chwalą się otrzymanym prawem jazdy, czy mandatem, na którym widnieje komplet danych osobowych. Monitorowaliśmy potencjalnie wrażliwe treści wrzucane przez internatów i ostrzegaliśmy ich o zagrożeniach. Dzięki temu wiele wrażliwych treści zostało usuniętych.

Dodatkowo w zakresie cyberbezpieczeństwa prowadzimy też szkolenia dla firm. Rozmawiamy, jak zabezpieczać się przed zagrożeniami i pokazujemy, jak działają przestępcy.

Na koniec zajrzyjmy w przyszłość. Jakie nowe zagrożenia przewiduje Pan dla funkcjonowania banków i klienta – użytkownika bankowości elektronicznej i mobilnej?

Wciąż groźny jest phishing i należy się spodziewać, że zarówno kwestie związane z obowiązywaniem unijnej dyrektywy, jak i podszywaniem się pod inne firmy i instytucje to tematy, które będą zajmować branżę cyberbezpieczeństwa w 2019 roku. Pojawią, a właściwie już pojawiają się także nowe wyzwania, które są bezpośrednio skorelowane z rozwojem technologii. Jednym z nich jest

bezpieczeństwo aplikacji mobilnych. Wyraźnie widać, że liczba użytkowników bankowych rozwiązań stale rośnie. IKO oferowane przez PKO Bank Polski ma już ponad 3 mln aktywnych aplikacji i pod tym względem jesteśmy liderem na rynku. Coraz większa popularność rozwiązań mobilnych to wyzwanie dla ich twórców, w tym także dla działów cyberbezpieczeństwa. Aplikacje muszą być bezpieczne, niezawodne i przyjazne dla klienta. Uzyskanie tych celów wymaga ścisłej współpracy biznesu, IT i bezpieczeństwa. Tym bardziej, że liczba innowacyjnych rozwiązań stale się zwiększa, a wraz z tym rośnie również liczba potencjalnych zagrożeń. Dobrym przykładem jest tutaj IoT. Do niedawna abstrakcyjnym mogło wydawać się włamanie przez hakera np. do inteligentnej lodówki czy autonomicznego samochodu. Cyberprzestępcy będą jednak szukać najsłabszych ogniw w całym systemie i z premedytacją je wykorzystywać. Już w tej chwili obserwujemy olbrzymi wzrost botnetów składających się z urządzeń IoT i ich wykorzystanie do ataków DDOS na wielką skalę. Troska o bezpieczeństwo Internetu rzeczy wraz ze wzrostem popularności tego typu rozwiązań będzie zatem bardzo istotnym zadaniem zespołów cyberbezpieństwa. Podobnie, jak wykorzystywanie w coraz większym zakresie sztucznej inteligencji, robotyzacji i uczenia maszynowego. Masowe ataki na te rozwiązania dopiero przed nami, ale już teraz warto zastanowić się nad nowym modelem zagrożeń i odpowiednio się do niego przygotować, bo potencjał tych rozwiązań może zostać wykorzystany także do budowania fałszywych modeli zachowań uniemożliwiających automatyczne wykrywanie anomalii oraz automatyzacji ataków. Rosnące znaczenie technologii zmusza do tego, żeby przemyśleć podejście do dbania o bezpieczeństwo. Dziś stawianie firewalli już nie wystarcza. To nie mury wokół zapewnią nam obronę przed atakami, ale dobre rozwiązania w detekcji i reagowaniu oraz stosowanie zasad „security by design” i „privacy by design”. Odpowiednie praktyki, stale podnoszona wiedza oraz mądra i skutecznie realizowana polityka bezpieczeństwa to dla wszystkich firm powinna być podstawa. Musimy zabezpieczać się na wielu frontach i maksymalnie ograniczyć słabe punkty we wdrażanych rozwiązaniach. Wykorzystując nowe technologie oraz nowe modele prowadzenia biznesu musimy jednocześnie pamiętać, że zmiany te generują również konieczność wprowadzenie zmian w obszarze cyberbezpieczeństwa, w tym przygotowania strategii zabezpieczenia nowych rozwiązań, np. chmury. W świetle realizowania przez PKO Bank Polski projektu Chmury Krajowej będzie to dla nas bez wątpienia duże wyzwanie w nadchodzącym roku. Tak jak udział w Programie Transformacji Cyfrowej wdrażanym w naszym banku.