DEKALOG BANKOWEGO CYBERBEZPIECZEŃSTWA WEDŁUG WICEPREZESA ZWIĄZKU BANKÓW POLSKICH [WYWIAD]

Według wiceprezesa Związku Banków Polskich Mieczysława Groszka operacje bankowe w sieci najlepiej przeprowadzać z jednego komputera, trzeba zmieniać co jakiś czas loginy i PIN-y oraz korzystać co najmniej z dwóch banków. To tylko niektóre punkty "dekalogu bezpieczeństwa" w bankowości elektronicznej. Zdaniem Groszka nie ma banku, który by nie spełniał podstawowych wymogów bezpieczeństwa elektronicznego.

PAP: Gdzie jest największy problem w cyberbezpieczeństwie systemu bankowego?

Mieczysław Groszek: Szkodliwość działań przestępczych jest widoczna w wielu obszarach. Problem w tym, że doskonaleniu się nowych technologii niemal równolegle towarzyszy rozwój "złych" technologii, tj. wykorzystywanych do nadużyć i przestępstw. Np. w Stanach Zjednoczonych najwyższą liczbę nadużyć odnotowuje się nie w bankowości, a w ubezpieczeniach. Chodzi tu o wykradanie danych osobowych, szczególnie tych wrażliwych, takich jak historia choroby i sprzedawanie ich ubezpieczycielom. W bankowości nacisk na ostrożność i bezpieczeństwo jest większa niż w innych sektorach, bo tu cybernadużycie przynosi skutki natychmiast odczuwalne. Ponadto jest duża przestrzeń do powstawania zagrożeń - mamy przecież 32 miliony rachunków internetowych i 35 milionów kart płatniczych. Te dwa obszary są bardzo narażone na ataki. Dlatego ważne jest dokładne zlokalizowanie segmentów, w których takie ataki mogą wystąpić.

Czy w związku z powszechnością kart płatniczych nadużyć tu jest najwięcej, czy może segment kart jest względnie bezpieczny, bo ludzie nauczyli się już z nich korzystać i przestrzegają procedur?

Niestety liczba nadużyć tu nie maleje. Najczęściej występują ich dwa rodzaje - przestępca może włamać się do bazy danych i wykraść dane właściciela karty, które może potem użyć. W Polsce na szczęście nie ma tego zjawiska, bo nie ma już u nas kart z tzw. paskiem, które były słabiej chronione. Dzisiaj karty są zabezpieczone przez chipy, co powoduje wyższy poziom ochrony. Liczba kart zresztą nie powiększa się, bo coraz powszechniejsze są płatności mobilne. Banki, które są wydawcami kart cały czas jednak pracują nad wzmocnieniem ich bezpieczeństwa. Zastrzeganie kart też staje się coraz łatwiejsze i bardziej powszechne - na przykład za pomocą numeru 828 828 828 zastrzeganych jest obecnie ok. 10 proc. kart, czyli ok. 100 tys. rocznie.

Bankowość internetowa tzw. zwykłemu człowiekowi wydaje się być trudniejsza do ochrony niż karty, bo tu dochodzi strach o działalność hakerów, którzy mogą wykradać pieniądze. Tak przynajmniej wiele osób motywuje niechęć do przechodzenia na bankowość internetową.

Statystyki tego nie potwierdzają. Oczywiście są ludzie, głównie ze średniej i starszej generacji, którzy mówią: nie, bo nie wiem, co się dzieje w cyberprzestrzeni. Ale na dużych liczbach to się nie potwierdza. Trzeba pamiętać, że bankowość internetowa zrobiła totalny przełom w tzw. customer experience, czyli formie doświadczenia klienta w kontakcie z bankiem. Jej rozwój dobrze ilustrują liczby. Jeśli chodzi o straty na bankowości elektronicznej wzrost między 2014 a 2015 roku był trzykrotny. W 2014 roku straty były 30 mln zł, a w 2015 roku 90 mln zł. Oczywiście kwota wydaje się duża, ale jeśli odnieść to do skali operacji, które są wykonywane i odnotowanego w tym sektorze w roku 2015 wzrostu, to wspomniane wysokości odpowiadają zaledwie 0,006 proc. ogółu depozytów. Podobnie w relacji do zysków banków to jest maleńka część. W tej sferze banki cały czas pracują, udoskonalając technologię i procedury bezpieczeństwa. Np. obserwują, ile czasu klient przechodzi przez stronę ostrzegającą o zagrożeniach. Jak widzą, że użytkownik tylko mechanicznie klika przycisk potwierdzający, że przeczytał ostrzeżenia, to zamiast zamieszczać 15 zasad bezpieczeństwa małym drukiem, wpisują przemiennie, dwie czy trzy, które klient ma większą szansę zobaczyć i przyswoić. Banki instalują też często za klientów oprogramowanie antywirusowe, bo wielu klientów nie aktualizuje u siebie tych programów na czas.

Czy "phishing" (oszustwo polegające na podszywaniu się pod inną osobę lub instytucję, by wyłudzić informację, np. fabrykowanie fałszywej strony bankowej, by uzyskać od osoby oszukiwanej login i hasło do banku - PAP) jest nadal częstym nadużyciem?

Zwyczaje w bankowości elektronicznej dopiero się kształtują i końcowy użytkownik powinien zawsze sobie uświadomić, jakie są skutki jego niestaranności. Np. właśnie instalowanie programów ochronnych powinno być bardziej staranne, bo często pod nieautoryzowanym hasłem zainstalowania programu antywirusowego kryje się właśnie "phishing".

Jak temu zapobiec?

Między innymi przez edukację. Postulowaliśmy np. by wpisać cyberbezpieczeństwo do podstawy programowej w szkołach. Ważne jest też zachowanie mediów, np. przy komentowaniu incydentów. Kilka lat temu media wznieciły obawy o karty zbliżeniowe, że np. łatwo te karty zeskanować, wystarczy że przejdzie się obok urządzenia skanującego. Wtedy przeprowadziliśmy akcję informacyjną, z której wynikało, że technicznie jest to możliwe, ale do tego trzeba mieć całe laboratorium. Jeśli więc chodzi o reakcję na incydenty - z jednej strony nie należy niepotrzebnie straszyć ludzi, a z drugiej właściwe "straszenie" może mieć pozytywny efekt, bo ludzie mogą zacząć zwracać większą uwagę na bezpieczeństwo. Straszenie musi być więc jakoś skalibrowane. Przed rokiem pojawiła się informacja, że 217 polskich banków komercyjnych i spółdzielczych zostanie zaatakowanych i podano nawet datę. To było w biuletynie jakiejś firmy, która dodawała, że przed tego rodzaju atakami chronią jej produkty. Takie postępowanie jest przykładem niedopuszczalnego nadużycia. Także publiczne komunikaty w takich sprawach powinno się redagować ostrożnie. Kiedyś ABW ostrzegła KNF, że może mieć miejsce fala cyberataków i KNF zamieścił na swojej stronie ostrzeżenie. Jednak było ono zbyt techniczne i przestraszyło ludzi, bo media podając je robiły to w otoczce sensacji, bez oceny potencjalnych zagrożeń. Od tego czasu zostały wydane ze cztery podobne alerty, ale KNF już tego nie publikował w taki sposób. Z kolei my, jako sektor bankowy, dwa lata temu mieliśmy ostrzeżenie o ataku na system, półtora miesiąca przed zdarzeniem. Z podaną datą atak nie nastąpił. Zrobiliśmy pełny alert, zaprosiliśmy Ministerstwo Cyfryzacji, KNF, ABW i to nie przeniknęło. Był to zatem stress test tego systemu. Ale przy tej okazji rozbudowaliśmy nasze procedury i w tym roku powołaliśmy bankowe centrum cyberbezpieczeństwa. Na stronie ZBP prowadzimy też zakładkę poświęconą cyberbezpieczeństwu pt. "bezpieczny bank". Zawieszamy tam nasze broszury i komentarze do zdarzeń.

Czytaj też: Wiceprezes Związku Banków Polskich: Cyberbezpieczeństwo jest wbudowane w DNA biznesu bankowego

Czy można banki różnicować pod względem procedur bezpieczeństwa?

Nie ma banku, który by nie spełniał podstawowych wymogów bezpieczeństwa elektronicznego. W tym zakresie podejście banków jest solidarne, bo tu nie ma między bankami konfliktu interesów. Tam gdzie w grę wchodzi bezpieczeństwo nie konkurujemy, tylko współdziałamy. Kolejnym strażnikiem naszego bezpieczeństwa jest KNF, która wydała dyrektywę D w sprawie bezpieczeństwa systemów IT w bankach, podnosząc rangę tej sfery. W myśl tej dyrektywy za cyberbezpieczeństwo nie jest odpowiedzialny już tylko dział IT, ale cały zarząd. KNF ma też zwiększone możliwości inspekcyjne. Może np. udawać klienta, zwracając uwagę na elementy bezpieczeństwa - jak klient jest sprawdzany, jak szybko jest otwierany rachunek itp.

Jakby pan miał wskazać jeden najbardziej słaby punkt?

Klient. Wiele osób np. nie zmienia nigdy loginów na strony bankowe. Właśnie dlatego klient jest często badany przez banki pod kątem uchybień w zakresie przestrzegania bezpieczeństwa.

Czy jest możliwość obejścia przez przestępców procedury otrzymywania hasła na telefon komórkowy?

Zdarzały się takie przypadki. Kiedyś jeden z telekomów wydawał duplikaty kart bez dowodu osobistego. Ktoś szykując "phishing" szedł więc do telekomu, mówił, że zgubił telefon i potrzebuje duplikat karty SIM i podawał numer tego, kogo chce "sphishować". Potem podkładał fałszywą stronę, sms przychodził na numer właściwy, ale ten numer właściwy był na tę chwilę podmieniony. Telekom orientował się, że jest zduplikowany numer i go wyłączał, ale "phishing" był skuteczny. Dlatego zwróciliśmy się do telekomów z uwagą, że nie można wydawać duplikatów kart na zasadzie oświadczenia, tylko trzeba sprawdzać dowody osobiste.

Jakby pan miał przedstawić dekalog użytkowników bankowości cyfrowej, to co by pan zalecił?

Po pierwsze - potraktować to poważnie na wejściu, przeczytać wszystko, co bank zaleca; po drugie - nie korzystać z każdego dostępnego urządzenia, najlepiej operacje bankowe przeprowadzać z jednego komputera; po trzecie - nie lekceważyć programów antywirusowych; po czwarte - zmieniać co jakiś czas loginy i PIN-y; po piąte - czytać to, co bank przekazuje w zakresie bezpieczeństwa; po szóste - korzystać co najmniej z dwóch banków; po siódme - starać się wyrobić własne kryteria oceny i nie ulegać plotkom; po ósme - ufać, że bezpieczeństwo klienta jest także bezpieczeństwem banku; po dziewiąte - mieć na uwadze, że cały czas te technologie rozwijają się; po dziesiąte, najbardziej oczywiste, w odniesieniu do kart - strzec ich i nie udostępniać nikomu PIN.

Rozmawiał Piotr Śmiłowicz (PAP)