Poradnik Bezpieczeństwa

Raiffeisen POLBANK
Z przyjemnością

CZYM JEST BANKOWOŚĆ MOBILNA I DLACZEGO WARTO Z NIEJ KORZYSTAĆ?

Bankowość mobilna jest jednym z elektronicznych kanałów dostępu do banku, wykorzystującym w charakterze terminali dostępu telefony komórkowe, a jako medium dostępowe, sieci operatorów telefonii komórkowej lub sieci bezprzewodowe – ogólnodostępne i prywatne. Bankowość mobilna cieszy się wciąż rosnącym zainteresowaniem Klientów. Klientami bankowości mobilnej stają się przede wszystkim osoby otwarte na innowacje, ceniące swobodę zarządzania swoim kontem w banku z każdego miejsca na świecie i o każdej porze doby.

Wszystko, czego potrzeba do korzystania z bankowości mobilnej, to odpowiedni telefon dostosowany technologicznie do wymagań aplikacji oferowanej przez bank. Nowoczesne smartfony, działające pod kontrolą systemów *Android i iPhone/iPad OS, Windows Phone*, a także starszych systemów *Symbian czy Windows Mobile*, spełniają minimalne wymagania takich aplikacji.

Z JAKIMI ZAGROŻENIAMI MUSI LICZYĆ SIĘ UŻYTKOWNIK BANKOWOŚCI MOBILNEJ?

Wraz z postępem technologicznym, telefon komórkowy w coraz większym stopniu upodabnia się do klasycznego komputera. Dzisiejsze smartfony mocą obliczeniową znacznie przewyższają komputery, które jeszcze kilka lat temu były używane do pracy czy zabawy. Obok rozlicznych korzyści, takich chociażby, jak coraz większa funkcjonalność urządzenia, uniwersalność jego zastosowań i przyjazność interakcji z użytkownikiem, ma to niestety także pewne negatywne skutki. Rośnie, bowiem poziom istotności i liczba zagrożeń, jakim użytkownik musi stawić czoło, chcąc, aby korzystanie z telefonu komórkowego jako uniwersalnego urządzenia komunikacji bezprzewodowej i dostępu do banku nadal pozostało czynnością bezpieczną. Charakter wspomnianych zagrożeń staje się coraz bliższy temu, czemu sprostać muszą stojące na biurku lub przenośne, klasyczne komputery podłączone do sieci.

BEZPIECZNE KORZYSTANIE Z BANKOWOŚCI MOBILNEJ JEST W ZNACZNYM STOPNIU ZALEŻNE OD BEZPIECZEŃSTWA NARZĘDZIA DOSTĘPOWEGO, JAKIM JEST TELEFON KOMÓRKOWY.

Tak, jak krytycznym czynnikiem decydującym o bezpieczeństwie korzystania z bankowości internetowej jest odpowiednie zabezpieczenie komputera użytkownika, analogicznie w bankowości mobilnej, równie ważne jest spełnienie minimalnych wymagań bezpieczeństwa w zakresie zabezpieczenia telefonu komórkowego oraz bezpiecznych praktyk jego stosowania.

Poważnym zagrożeniem dla użytkowników smartfonów jest *oprogramowanie złośliwe* takie jak wirusy, robaki internetowe, oprogramowanie szpiegujące, wytrychy czy konie trojańskie. Już teraz, pod pojęciem bezpiecznego smartfona rozumie się takie urządzenie, które obowiązkowo posiada zainstalowane dobre oprogramowanie *antymalware*.

Skala zjawiska tworzenia i propagowania oprogramowania złośliwego przeznaczonego do infekowania telefonów komórkowych jeszcze, co prawda, nie jest tak duża jak w przypadku komputerów, ale wykazuje stałą tendencję wzrostową. Ze stałym wzrostem tego typu zagrożenia należy się więc liczyć.

Zagrożenie, wynikające z infekcji telefonu oprogramowaniem złośliwym ma dokładnie taki sam charakter jak dobrze znane zagrożenia w świecie klasycznych komputerów. Zainfekowanie telefonu oznacza ryzyko kradzieży poświadczeń tożsamości (loginów i haseł dostępowych) nie tylko w bankowości mobilnej (także na przykład do systemów poczty i portali społecznościowych), ujawnienia numerów kart kredytowych, PIN-ów i innych wrażliwych danych. Na tym jednak nie koniec. Infekcja telefonu w pewnych przypadkach wiąże się także z poważnym ryzykiem podmiany danych transakcyjnych (na przykład kont beneficjentów zlecanych przelewów). Mowa tu oczywiście o klasycznych środkach z arsenału ataków należących do kategorii ***man-in-the-browser***. Na szczęście jednak to zagrożenie nie dotyczy klientów bankowości mobilnej Raiffeisen Bank Polska S.A., bowiem aplikacja udostępniana przez bank jest w pełni niezależna od przeglądarki.

Trzeba ponadto nieustająco pamiętać, iż **telefon komórkowy wyposażony w interfejsy sieciowe w postaci wbudowanego modemu GSM lub bezprzewodowej karty sieciowej (WiFi), od chwili nawiązania połączenia z siecią Internet, staje się takim samym, wyeksponowanym na ataki, elementem globalnej sieci jak klasyczny komputer.** Jest zatem potencjalnym celem ataków ze strony hakerów, ***botnetów*** czy oprogramowania złośliwego. Nie powinna więc podlegać dyskusji potrzeba wyposażenia go w skuteczną osobistą zaporę sieciową.

Brak ochrony przed atakami z sieci Internet może skutkować na przykład infekcją telefonu oprogramowaniem złośliwym ze wszystkimi tego szkodliwymi skutkami (także dla bankowości mobilnej), opisanymi wcześniej lub wyprowadzeniem poufnych danych. Środkiem zaradczym jest instalacja na smartfonie zintegrowanego pakietu zabezpieczeń, obejmującego jako minimum skaner antywirusowy i osobistą zaporę sieciową. Dostępne na rynku produkty tego rodzaju na ogół oferują dodatkowo ochronę na poziomie kontroli procesów, przeciwdziałania atakom z sieci Internet i czasem także możliwość szyfrowania plików.

Przyjmując słuszne założenie, iż telefon komórkowy jest wymagającym ochrony urządzeniem komputerowym, nie należy instalować na nim **oprogramowania z niezaufanych źródeł** (na przykład nielegalnego oprogramowania poddanego przeróbkom w celu złamania zabezpieczeń praw autorskich i licencyjnych). Pamiętajmy, że takie oprogramowanie nierzadko posiada wbudowane w kod funkcje tylnych wejść (ang: backdoors), które mogą być wykorzystane przez agresorów do złamania zabezpieczeń telefonu, wygenerowania wysokich rachunków za transfer danych, zainstalowania oprogramowania złośliwego albo - najzwyczajniej - wyprowadzenia wrażliwych danych z pamięci telefonu.

Nie należy zapominać także o tym, że źle napisana aplikacja często przyczynia się do osłabienia mechanizmów bezpieczeństwa telefonu, ponieważ jej podatności eksponują dodatkowo także system operacyjny i inne oprogramowanie narzędziowe i użytkowe zainstalowane na telefonie na atak agresorów, a wszak, nie od dziś wiadomo, iż o bezpieczeństwie całości dowolnego rozwiązania zawsze decyduje najsłabsze ogniwo w łańcuchu jego zabezpieczeń. Aplikacje instalowane na telefonie powinny być podpisane cyfrowo przez dostawcę. Podpis cyfrowy pozwala na zweryfikowanie pochodzenia aplikacji (od zaufanego dostawcy) i jej integralności (nikt nie ingerował w jej kod od momentu jej skompilowania przez zaufanego dostawcę).

Konsekwencją instalacji aplikacji z niezaufanych źródeł może być osłabienie mechanizmów zabezpieczeń telefonu (w postaci na przykład aktywacji tylnego wejścia, umożliwiającego przejęcie zdalnej kontroli nad urządzeniem, czy wyłączenie mechanizmów zabezpieczeń, takich jak osobista zapora sieciowa oraz skaner antywirusowy), wprowadzenie nowych podatności, z których każda jest potencjalnym celem ataku możliwego do przeprowadzenia z sieci Internet. Wobec tego, co zostało napisane, zbędnym wydaje się dalsze opisywanie szkodliwych konsekwencji instalacji na smartfonie niezaufanego oprogramowania dla bezpieczeństwa korzystania z bankowości mobilnej.

Raiffeisen POLBANK
Z przyjemnością

Jednym z najpoważniejszych źródeł podatności i luk w bezpieczeństwie każdego rodzaju oprogramowania są jego, różnego rodzaju, usterki i wady. Przeważnie są to wady istniejące na poziomie kodu aplikacji. Producenci oprogramowania usuwają ujawnione w nim błędy i usterki poprzez opracowywanie oraz dystrybucję do użytkowników odpowiednich poprawek i aktualizacji czyli *„łatek" (ang: patches).*

System operacyjny telefonu wraz z oprogramowaniem standardowym wymaga okresowych aktualizacji, korygujących błędy oraz usuwający podatności i luki w bezpieczeństwie. Dotyczy to zwłaszcza otwartych platform np. *Android.* Na szczęście w przypadku dominujących na rynku systemów operacyjnych *(Android, iOS, Windows Phone)* aktualizacja oprogramowania jest prosta i bardzo często automatyczna. Należy jednak podkreślić, że obowiązkiem użytkownika, przed podjęciem ewentualnej decyzji o aktualizacji oprogramowania systemowego jest przygotowanie kopii zapasowej danych telefonu.

Aktualizację można przeprowadzić we własnym zakresie jedynie wówczas jeśli jest to operacja bezpieczna użytkownik wie jak ją przeprowadzić, ma do dyspozycji odpowiednie narzędzia w postaci przeznaczonego do tego celu oprogramowania narzędziowego od producenta telefonu, właściwe akcesoria (jak choćby kable do podłączenia telefonu do komputera), aktualizacja oprogramowania pochodzi z wiarygodnego źródła (od producenta telefonu), operacja aktualizacji nie narusza warunków gwarancji czy jakichkolwiek warunków ewentualnych umów licencyjnych, zostały przygotowane wcześniej (i przetestowane) kopie zapasowe danych z telefonu. W przypadku, kiedy użytkownik nie jest w stanie z powodzenie przeprowadzić wszystkich czynności aktualizacji, powinien rozważyć możliwość zlecenia tego specjalistycznej firmie usługowej.

Czy i ewentualnie jak często należy takie aktualizacje przeprowadzać, to oczywiście zależy od konkretnej platformy programowej smartfona. Prawidłowością jest, że otwarte platformy, nie związane z jednym konkretnym producentem skupiają na sobie większe zainteresowanie - nie tylko legalnie działających ekspertów od wykrywania podatności ale także świata hakerskiego. Zalecane jest śledzenie doniesień o bezpieczeństwie wykorzystywanego przez siebie rodzaju smartfona i instalowanie aktualizacji i łatek zalecanych przez producentów.

Kolejnym ważnym czynnikiem decydującym o bezpieczeństwie telefonu i zapisanych w jego pamięci danych jest jego ochrona przed zagubieniem czy kradzieżą. Wrażliwe dane (na przykład hasła, numery kart kredytowych, numery PIN itp.) zapisane w pamięci telefonu lub na karcie pamięci muszą być zabezpieczone przed ujawnieniem niepowołanym osobom. W praktyce zabezpieczenia takie sprowadzają się do zaszyfrowania tych danych. Na rynku dostępnych jest wiele komercyjnych produktów oferujących szyfrowanie wrażliwych danych przechowywanych w telefonie. Są tez dostępne, nie mniej skuteczne, rozwiązania darmowe.

Nie tracą na aktualności także takie podstawowe zasady jak niepozostawianie telefonu bez nadzoru (na przykład w samochodzie albo w kieszeni płaszcza w publicznej szatni, w środkach komunikacji, w pokojach hotelowych itp.) oraz bezpieczne przenoszenie telefonu (w taki sposób, aby nie wypadł lub nie został wyciągnięty z kieszeni przez złodzieja). Zagubienie lub kradzież telefonu z niezabezpieczonymi danymi może mieć dla właściciela smartfonu fatalne skutki.

APLIKACJA CZY LEKKA STRONA WWW?

Raiffeisen POLBANK
Z przyjemnością

Posiadacze smartfonów chcący przy użyciu tych właśnie urządzeń uzyskać dostęp do zgromadzonych przez siebie środków finansowych za pośrednictwem internetu, stają obecnie przed wyborem pomiędzy dwoma typami rozwiązań – mobilnej bankowości opartej o oprogramowanie niezależne od przeglądarki internetowej, tzw. „grubego klienta" np. aplikacja Mobilny Bank bądź dostępu w oparciu o tzw. „lekki" serwis WWW za pośrednictwem przeglądarki zainstalowanej w telefonie (czyli tzw. *„light web browsing"*). Wyboru pomiędzy tymi rozwiązaniami warto dokonywać świadomie mając na uwadze to, jaką każde z nich wykazuje podatność na zagrożenia charakterystyczne dla mobilnych kanałów dostępu. Przedstawiony poniżej model zagrożeń oraz charakterystyka każdego z rozwiązań pomoże w ich ocenie pod kątem bezpieczeństwa.

Zagrożenie	**Aplikacja oparta o niezależne oprogramowanie („grubego klienta") – Mobliny Bank**	**Dostęp oparty o przeglądarkę Web (web browsing) w telefonie**
„Podsłuch" sieciowy, przez agresorów, wrażliwych danych (utrata poufności danych) przez zastosowanie narzędzi do rejestracji ruchu na łączach sieci (tzw. sniffery) oraz serwerów pośredniczących (serwery Proxy).	**małe ryzyko**	**duże ryzyko (z uwagi na łatwość ataku)**
Atak man-in-the-middle („podsłuch" oraz naruszenie integralności danych) – ingerowanie w strumień danych w sesji (na przykład podmiana elementów transakcji) – typowe dla 'modus operandi' aktualnie wykorzystywanego przez przestępców oprogramowania złośliwego.	**małe ryzyko**	**duże ryzyko**
Oprogramowanie złośliwe, infekujące telefon, przechwytujące poświadczenia tożsamości użytkownika.	**małe ryzyko**	**duże ryzyko**
Oprogramowanie złośliwe odpowiedzialne za przekierowania do fałszywych stron banków internetowych	**praktyczny brak ryzyka**	**duże ryzyko**
Podmiana treści stron internetowych	**praktyczny brak ryzyka**	**duże ryzyko**
Przekierowania do fałszywych serwerów bankowości internetowej	**praktyczny brak ryzyka**	**duże ryzyko**

NIEZALEŻNE OD PRZEGLĄDARKI INTERNETOWEJ OPROGRAMOWANIE „GRUBEGO KLIENTA" NA TELEFON KOMÓRKOWY CHARAKTERYZUJE SIĘ:

- możliwością łatwego i wiarygodnego uwierzytelnienia źródła pochodzenia aplikacji (zagwarantowanie, że 'uzłośliwiona' przez hackerów aplikacja nie została podstawiona w miejsce legalnej aplikacji) oraz zagwarantowania jej integralności (aplikacja nie została zmodyfikowana na przykład w celach ataku). Wszystko to dzięki zastosowaniu podpisu elektronicznego kodu oprogramowania i jego późniejszej weryfikacji;

- możliwością kryptograficznego, dwustronnego (wzajemnego) uwierzytelnienia aplikacji klienta i serwera (obie strony – klient i serwer – łącząc się z sobą, mogą sobie wzajem zaufać);

- niezależnością aplikacji od przeglądarki i przez to uzyskaniem odporności na typowe ataki, charakterystyczne dla aplikacji webowej (ataki z kategorii *client side attack*, czyli ataki, których celem jest nie bank lecz komputer klienta), w tym kradzież poświadczeń tożsamości (haseł, kodów itp), czyli tzw. *phishing*;

- szyfrowaniem informacji nieprzerwanie na całej ścieżce jej przesyłania: od aplikacji klienta do serwera *(end-to-end)*. Brak na tej ścieżce jakichkolwiek serwerów pośredniczących (proxy) oznacza praktyczny brak ryzyka „podsłuchu", ataków typu *man-in-the-middle*, ujawnienia, czy przestępczego wykorzystania przechwyconych poświadczeń tożsamości użytkownika;

DOSTĘP OPARTY O 'WEB BROWSING' I PRZEGLĄDARKI W TELEFONIE POSIADA NASTĘPUJĄCE CECHY:

Raiffeisen POLBANK
Z przyjemnością

- Aplikacja dziedziczy błędy i luki w bezpieczeństwie zastosowanej przeglądarki internetowej. Luki te wynikają zazwyczaj z błędów w kodzie przeglądarek, a – wato w tym miejscu dodać - błędów tych jest sporo. Są wśród nich też krytyczne błędy, „niełatane" przez producentów od – wręcz - kilku lat. Spora ich część wynika także ze słabości konfiguracji przeglądarki.

- Poważne ryzyko ataków ***phishingowych***, tym większe, że najskuteczniejsze z nich opierają swoje działanie na przekierowaniach do fałszywych stron banków, na „podsłuchu" klawiatury ***(keylogging)*** oraz, tym samym, śledzeniu przy użyciu oprogramowania złośliwego, dialogu użytkownika z serwerem banku. Zauważyć wypada w tym punkcie, że bardzo niewielu użytkowników smartfonów wyposaża swoje urządzenia w oprogramowanie antywirusowe, które mogłyby potencjalnie to zagrożenie zmniejszyć.

- Przeglądarka *Opera Mini i Opera Mobile*, rekomendowane przez niektóre banki, działają w oparciu o serwer pośredniczący, na którym wszystkie dane wymieniane pomiędzy użytkownikiem, w tym dane o tożsamości użytkownika (hasła, PIN-y itp.), a bankiem, pojawiają się w postaci niezaszyfrowanej – jawnym tekstem. Zatem bezpieczeństwo takiej formy komunikacji bazuje na założeniu, że informacja nie ma szans wypłynąć z serwerów pośredniczących, co stanowi założenie poczynione mocno na wyrost, wziąwszy pod uwagę choćby incydenty ze spektakularnymi wyciekami danych, ujawnionymi następnie w serwisie *Wikileaks*.

W świetle przedstawionych argumentów rysuje się istotna przewaga rozwiązań dostępu do bankowości mobilnej za pośrednictwem aplikacji („grubego klienta"), a przywoływana niekiedy przez użytkowników konieczność rzekomo kłopotliwej instalacji niezależnej od przeglądarki internetowej, oddzielnej aplikacji na telefonie komórkowym, jawi się jedynie jako niewiele znacząca, drobna niedogodność, którą warto pokonać, bo w nagrodę użytkownik otrzymuje **dużo większe bezpieczeństwo, niż w przypadku dostępu poprzez interfejs przeglądarki internetowej w telefonie.**