O krok przed cyberzłodziejem

Hakerzy dotarli pod strzechy. Dosłownie każdy z nas może znaleźć się na celowniku internetowych oszustów, których liczba systematycznie się powiększa.

Cyberprzestępczość przestała być już domeną zbuntowanych geniuszy czy złowrogich gangów; przeprowadzenie udanego ataku leży w zasięgu zwykłego studenta informatyki. W efekcie każdego dnia można spotkać się z najróżniejszymi zagrożeniami – najczęściej, rzecz jasna, nie zdając sobie z tego sprawy.

Otrzymałeś e-mail z informacją o atrakcyjnej wygranej, chociaż nigdy nie uczestniczyłeś w żadnym konkursie? Z reguły nie jest to tylko nachalny i denerwujący spam. Otwarcie takiej wiadomości – a w szczególności zawartego w niej załącznika – może skutkować zainstalowaniem na komputerze złośliwego oprogramowania (malware). Spora część oprogramowania malwarowego ma za cel przejęcie kontroli nad kontami bankowymi użytkowników, z reguły poprzez przechwycenie kodów dostępu do rachunku. Zdarzają się i takie programy, które są w stanie bez wiedzy użytkownika podmienić numer rachunku bankowego na inny. Jeżeli, wysyłając przelew, uzupełniasz numer konta odbiorcy metodą kopiuj-wklej, malware wstawi rachunek należący do cyberprzestępcy. O dokonanym oszustwie dowiesz się z reguły z chwilą otrzymania wezwania do zapłaty za usługi od właściwego usługodawcy.
Inną dość popularną formą elektronicznej przestępczości jest phishing. Istotą ataku phishingowego jest rozsyłanie e-maili z adresu internetowego do złudzenia przypominającego domenę należącą do instytucji zaufanych. Cyberzłodzieje podszywają się pod banki, biura pośrednictwa pracy, a nawet urzędy skarbowe. Jeśli drogą mailową otrzymamy podejrzaną fakturę za usługi, z których nie korzystaliśmy, czy wezwanie do zapłaty z tytułu niesprecyzowanego zadłużenia – niemal na pewno mamy do czynienia z próbą wyłudzenia. Bardziej zaawansowane formy phishingu mają skłonić odbiorcę trefnej przesyłki do przesłania numeru karty kredytowej, jej daty ważności i kodu CVC – w konsekwencji złodziej, dysponując wyłudzonymi danymi, może dokonywać zakupów na koszt właściciela karty. Bardziej zaawansowaną grupą phishingu jest spear phishing; o ile tradycyjny atak phishingowy polega na masowym mailingu metodą chybił-trafił, to spear phishing ukierunkowany jest na określone osoby lub środowiska. Takie e-maile mogą być adresowane imieniem, nazwiskiem oraz adresem odbiorcy, nazwą prowadzonej przez niego firmy, jak również zawierać dodatkowe dane (np. numer rejestracyjny samochodu należącego do właściciela skrzynki mailowej w fikcyjnym blankiecie polisy ubezpieczeniowej). Dość powszechną formą przestępczości internetowej są również wyłudzenia dokonywane w transakcjach handlowych. Z reguły polegają one na wyłudzaniu przedpłaty za towary lub usługi w internetowych serwisach aukcyjnych i ogłoszeniowych. Niekiedy w ten sam sposób złodzieje wyłudzają na przykład dane karty kredytowej.

W jaki sposób uniknąć oszustwa? Zabezpieczenia dostarczane wraz z produktami bankowymi, jak tokeny, karty kodów jednorazowych czy uwierzytelnianie SMS, choć spełniają najbardziej wyśrubowane standardy i wymogi prawno-regulacyjne (określone między innymi w Rekomendacji D KNF), nie są w stanie zapewnić pełnego bezpieczeństwa,bez współpracy ze strony klienta. Praktycznie żaden system zabezpieczający nie jest w stanie skutecznie zapobiec phishingowi. Dokonanie oszukańczej transakcji jest w tym przypadku głównie efektem psychologicznego zmanipulowania użytkownika bez udziału złośliwego oprogramowania. Banki z reguły blokują wprawdzie rachunki „podejrzane", wykorzystywane do wyłudzeń w sieci, a międzybankowy System Wymiany Ostrzeżeń o Zagrożeniach ułatwia przekazywanie informacji do innych placówek bankowych – jednak w miejsce jednego rachunku zidentyfikowanego jako niebezpieczny z reguły pojawia się kilka nowych. Również w przypadku złośliwego oprogamowania o wystarczającym poziomie zabezpieczeń mówić można jedynie w sytuacji, kiedy użytkownik zachowuje zasady bezpieczeństwa w korzystaniu z bankowości elektronicznej czy też mobilnej.

Do zwiększenia bezpieczeństwa transakcji dokonywanych online możemy się przyczynić na dwa sposoby. Pierwszy z nich to ostrożność i rozwaga podczas korzystania z sieci. Odradza się korzystanie z systemu transakcyjnego bankowości elektronicznej w przypadkowych miejscach, takich jak

internetowe kawiarenki, komputery w ośrodkach wczasowych czy sprzęt rodziny i kolegów – zwłaszcza w sytuacji, kiedy nie uzyskamy informacji o zainstalowanych zabezpieczeniach. Szczególną ostrożność zaleca się zachować w odbieraniu poczty elektronicznej; podejrzanie wyglądającą wiadomość lepiej od razu skasować, aniżeli doprowadzić do zainfekowania systemu. Analogiczna zasada dotyczy pobierania oprogramowania z sieci; umieszczone na popularnych torrentach filmy czy utwory muzyczne nie tylko pochodzą z nielegalnego źródła, ale też dodatkowo mogą być zainfekowane złośliwym oprogramowaniem. Zalecane jest korzystanie tylko z pewnych i sprawdzonych źródeł pobierania plików – na przykład oficjalnych stron rekomendowanych przez dystrybutorów (dotyczy to również oprogramowania darmowego!). Kończąc pracę w systemie bankowości elektronicznej, należy bezwzględnie się wylogować; zamknięcie okna przegladarki powoduje, że jeszcze przez kilka minut istnieje dostęp z poziomu urządzenia do rachunku bankowego – co ułatwia życie złodziejom.

Nie należy wysyłać tzw. przelewów autoryzujących, jeżeli nie mamy pewności co do odbiorcy przelewu. Przestępcy domagają się wysłania takiego przelewu pod pozorem weryfikacji danych klienta – na przykład przy zamieszczaniu ogłoszenia o poszukiwaniu pracy. W rzeczywistości dokonanie przelewu skutkuje otwarciem rachunku bankowego – a pełną kontrolę nad tym kontem przejmuje tylko i wyłącznie złodziej. Konto takie może posłużyć do wyłudzenia kredytu bankowego bądź też dokonywania innych przestępstw, jak choćby oszustw w handlu internetowym, a wszelkie kroki prawne będą w pierwszej kolejności kierowane przeciwko osobie figurującej w dokumentach jako właściciel konta!

Drugim, nie mniej istotnym kierunkiem działań jest zapewnienie bezpieczeństwa posiadanego sprzętu. Minimalnym wymaganym zabezpieczeniem jest oczywiście system antywirusowy, a jeśli korzystamy z programu pocztowego, jak Mozilla Thunderbird czy Microsoft Outlook – również odpowiedni filtr antyspamowy. Bezpieczeństwo urządzeń elektronicznych, w tym smartfonów, w istotny sposób zwiększa regularne instalowanie aktualizacji systemów operacyjnych, przeglądarek internetowych oraz wszystkich aplikacji, które służą do przeprowadzania operacji bankowych. Aktualizacji musi podlegać również system antywirusowy.

Karol Jerzy Mórawski

Zasady bezpiecznego dostępu i wykonywania transakcji:

- połączenie z Internetem musi być bezpieczne (unikaj łączenia się z publicznej sieci WiFi)
- trzeba uważać na fałszywe certyfikaty bezpieczeństwa np. rozsyłane przy pomocy poczty elektronicznej
- należy zawsze korzystać z aktualnych wersji systemu operacyjnego, oprogramowania antywirusowego i przeglądarki internetowej
- system pocztowy powinien być chroniony przed przychodzącym spamem. Wiadomości e-mail to jedna z najpopularniejszych dróg, jaką mogą do systemu pocztowego trafić wirusy i informacje, których celem jest wyłudzenie poufnych danych
- nie należy logować się do systemu e25 korzystając z odnośników otrzymanych pocztą elektroniczną lub znajdujących się na stronach nienależących do Banku
- należy unikać logowania z komputerów, do których dostęp mają również inne osoby (np. w kawiarenkach lub u znajomych)
- zalecane jest ręczne wpisywanie danych do zlecenia przelewu np. numerów rachunków, należy unikać wprowadzania numerów rachunków stosowania metody kopiuj/wklej
- nie należy instalować oprogramowania pochodzącego z nieznanych źródeł na komputerze, na którym korzysta się z bankowości internetowej
- należy zawsze kończyć pracę z systemem bankowości internetowej na komputerze korzystając z polecenia - wyloguj
- w przypadku wątpliwości co do prawidłowego działania bankowości internetowej lub stwierdzenia utraty środków należy niezwłocznie skontaktować się z Bankiem

Pamiętaj, że Bank nigdy nie prosi o:

- ✓ instalację certyfikatów na komputerach i telefonach komórkowych
- ✓ podanie danych kart płatniczych i kredytowych (numer karty, kod PIN) oraz danych dotyczących Twojego telefonu (numer i model)
- ✓ udział w testowaniu nowych funkcjonalności serwisu transakcyjnego
- ✓ wykonanie przelewów testowych ani zwrot środków na rachunki innych Klientów