Materiał pomocniczy nr 3

„Cyberbezpieczeństwo" - jak dbać o swoje pieniądze w sieci?

W ostatnich latach znacząco wzrosły zagrożenia związane z technologiami cyfrowymi. Najbardziej spektakularnym przykładem był atak, który nastąpił 12 maja tego roku. Cyberprzestępcy za pomocą robaka ransomware o nazwie **WannaCry** zainfekowali ok. 300 tysięcy komputerów lub systemów, paraliżując brytyjską służbę zdrowia, Nissana, Telefonicę, FedEx, rosyjskie banki i koleje państwowe, indyjskie linie lotnicze Shaheen Airlines oraz włoskie uniwersytety – w sumie instytucje w **150 krajach.** Wg informacji CERT Polska ofiarami tego wirusa padło ponad 1000 urządzeń w Polsce. Specjaliści IT analizujący cyberataki sygnalizują, że większość ataków ma 2 cele: finansowy oraz uzyskanie rozgłosu medialnego.

Przestępcy cały czas rozwijają narzędzia, wykorzystują różne metody socjotechniczne. Daje się zauważyć, że grupy te profesjonalizują się i działają na wzór niewielkich przedsiębiorstw. Uderzają tam, gdzie zarobek jest najłatwiejszy. Dlatego też widać większe zainteresowanie atakowaniem osób wykorzystujących komputery w domu, między innymi do korzystania z usług bankowości elektronicznej. Ataki są coraz bardziej zaawansowane i dotykają coraz to nowych obszarów. Jak choćby Internetu rzeczy. Infekowane są rzeczy codziennego użytku, jak kamery, lodówki czy systemy ochrony, ale także aplikacje, z których na co dzień korzystamy. Eksperci przewidują, że do 2020 roku na świecie będzie 200 mld połączonych urządzeń. Szybkie tempo rozwoju technologii **IoT** (Internet of Things – urządzenia podłączone do sieci Internet typu dekodery cyfrowe, kamery, telewizory, urządzenia sterujące), słabe zabezpieczenia tych urządzeń, brak cyklicznych aktualizacji zabezpieczeń – sprawiają, że stają się łatwym celem.

Człowiek jest najsłabszym ogniwem w całym cyklu ataku, a popełniane przez nas błędy ułatwiają lub umożliwiają skuteczne ataki cyberprzestępców.

Działania ułatwia przestępcom fakt, że klienci mają duże zaufanie do komunikacji wysyłanej z banku lub z logo banku. W dobie rozwoju technologicznego podrabianie dokumentów lub korespondencji elektronicznej jest bardzo proste i klienci powinni zwracać większą uwagę na to, jakie dokumenty i od kogo otrzymują. Przestępcy posługują się wirusami podmieniającymi nr rachunku, wyłudzaniem haseł czy wreszcie – podszywając się pod kontrahenta ofiary – wysyłają informacje o zmianie numeru rachunku.

Dlatego ważne jest, aby edukować o zagrożeniach. To klient pierwszy „widzi" fałszywą stronę lub jest atakowany różnymi metodami socjotechnicznymi. Odpowiednio wyedukowany klient ma większą

szanse wykryć niezgodności, uchronić się przed przestępstwem, nie reagując na próbę wyłudzenia, i powiadomić o zagrożeniu. Edukacja powinna być skierowana do różnych grup wiekowych i uwzględniać poziom wiedzy informatycznej odbiorców.

Ważne zasady:

Zwracaj uwagę na wygląd stron usług bankowości elektronicznej, komunikaty i powiadomienia w trakcie logowania i podczas korzystania z usług. Wszystkie inne niż standardowe zachowania, typu komunikaty o oczekiwaniu na połączenie, powinny budzić niepokój.

Pamiętaj, że smsKod lub wezwanie z tokena służą wyłącznie do potwierdzenia realizacji dyspozycji! Bank nie prosi o jego podanie w innych sytuacjach.

Nie instaluj i nie aktualizuj oprogramowania z innych źródeł niż sklepy z aplikacjami i oficjalne strony producenta.

Sprawdzaj zgodność numeru rachunku odbiorcy przed potwierdzeniem transakcji (smsKodem, tokenem).

Zwracaj uwagę na opis typu transakcji, numer rachunku, kwotę i dane odbiorcy podane w treści smsKodu potwierdzającego daną płatność.

Nie otwieraj wiadomości e-mail pochodzących od nieznanych adresatów, jak i przesyłanych w treści linków oraz załączników.

Loguj się do swojej bankowości internetowej tylko przez stronę banku lub korzystaj z zapisanych wcześniej linków.

Sprawdzaj, czy na pasku adresu usług bankowości elektronicznej znajduje się kłódka i opis certyfikatu wskazuje na właściciela strony np. bank.

Dbaj o to, aby oprogramowanie na Twoim urządzeniu było aktualne i legalne.

Korzystaj z bezpiecznej sieci internetowej zachowaj ostrożność, korzystając z bezpłatnych i nieznanych sieci WiFi.

Chroń swoje dane do logowania.

Włącz obrazek, który pokazuje się na stronie logowania po wprowadzeniu NIK (nazwy użytkownika).

Pamiętaj, aby wyłączyć „Bluetooth", jeśli obecnie z niego nie korzystasz.

Nie udostępniaj urządzeń, z których korzystasz, osobom postronnym.

Regularnie poszerzaj swoją wiedzę na temat istniejących zagrożeń.

Źródła:

https://www.bzwbk.pl/bankowosc-elektroniczna/bezpieczenstwo-i-prywatnosc/zelazne-zasady-bezpieczenstwa.html

https://www.bzwbk.pl/informacje-o-banku/biuro-prasowe/aktualnosci/bezpieczne-finanse-na-wakacjach-o-czym-pamietac.html

https://www.bzwbk.pl/bankowosc-elektroniczna/bezpieczenstwo-i-prywatnosc/bezpieczenstwo-bzwbk24-mobile.html#bezpieczenstwo-bzwbk24-mobile

https://www.bzwbk.pl/przydatne-informacje/pytania-i-odpowiedzi/karty-platnicze/pytania-i-odpowiedzi-karty-platnicze.html#transakcje_kartami_platniczymi

https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-internetowa

https://zbp.pl/dla-konsumentow/bezpieczny-bank/karty-bankowe

https://zbp.pl/dla-konsumentow/bezpieczny-bank/bankowosc-telefoniczna