BANK SPÓŁDZIELCZY W TOMASZOWIE LUBELSKIM
22-600 TOMASZÓW LUBELSKI UL. ELIZY ORZESZKOWEJ 2
tel. (084) 664 34 31, (084) 664 44 28, (084) 664 44 29, fax (084) 664 34 85

Informacja na temat zagrożeń związanych z korzystaniem z bankowości elektronicznej.

W związku z nasilającymi się atakami różnego typu na klientów bankowości elektronicznej pragniemy zwrócić Państwu uwagę na pojawiające się nowe zagrożenia oraz możliwości ich przeciwdziałania.
Uwagi oraz zalecenia podnoszące odporność systemu na ewentualne ataki złośliwego oprogramowania:

1. Aktualne oprogramowanie antywirusowe z włączoną opcją pełnego, okresowego skanowania komputera.
2. Sprawdzenie przed logowaniem czy wykorzystywane jest połączenie szyfrowane ("zatrzaśnięta kłódka" w pasku przeglądarki).
3. Prosimy zwrócić szczególną uwagę na nietypowe zachowanie się systemu bankowości elektronicznej, zwłaszcza przy logowaniu. Przykładem takiego zachowania może być komunikat o błędnym logowaniu w przypadku gdy jesteśmy pewni, że podaliśmy prawidłowy ID i klucz. Sytuacja taka może byś wynikiem działania złośliwego oprogramowania TINBA i VAWTRAK opisanego na stronie Związku Banków Polskich (ZBP) (szczegółowe informacje o zagrożeniu można sprawdzić na stronie http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci). Na podanej stronie ZBP opisuje jak Użytkownik powinien się zachować, w przypadku gdy dostrzeże nietypowe działanie bankowości elektronicznej.
4. Istnieje możliwość włączenia funkcjonalności polegającej na weryfikacji IP komputera użytkownika. Uruchomienie niniejszej usługi pozwoli zabezpieczyć Państwa przed logowaniem do bankowości z innych niż dozwolone przez operatora adresy IP, tzn. logowanie będzie możliwe tylko z pracy bądź tylko z domu (z określonej lokalizacji). Zapobiegnie to nieautoryzowanemu logowaniu się do systemu z innych lokalizacji przez oprogramowanie złośliwe.
5. Istnieje nowa metoda identyfikacji i autoryzacji w bankowości korporacyjnej (dla klientów posługujących się kartami elektronicznymi) – tokeny Vasco, która dzięki zastosowaniu mechanizmu „podwójnego klucza”, czyli innego hasła do logowania a innego do autoryzacji, gwarantuje wysoki poziom bezpieczeństwa, chroniąc przed takimi incydentami jak podmiany stron do logowania.
6. Została wprowadzona modyfikacja polegająca na autoryzacji edycji zdefiniowanych kontrahentów, odbiorców oraz szablonów przelewów. Zwiększa ona bezpieczeństwo w sytuacji braku szczegółowej kontroli numeru NRB przez użytkownika, bądź działania oprogramowania złośliwego. Po wprowadzeniu niniejszej modyfikacji każda zmiana nazwy lub numeru NRB zdefiniowanego odbiorcy, kontrahenta lub szablonu przelewu wymaga ponownej autoryzacji przez użytkownika. W związku z powyższym klienci w pierwszej kolejności powinni najpierw zdefiniować odbiorcę a następnie wprowadzić dla niego przelew (postępować tak należy również z przelewami jednorazowymi).
7. Została wprowadzona funkcjonalność umożliwiająca zablokowanie zmiany numeru NRB na wprowadzonych do systemu bankowości korporacyjnej przelewach (dot. klientów posługujących się kartami przy autoryzacji). W przypadku gdy klient wprowadzi przelew ręcznie lub zaimportuje go z pliku, jakakolwiek jego zmiana, bądź usunięcie przelewu wymaga dodatkowej autoryzacji. Jest to zabezpieczenie przed nieuprawnioną zmianą numeru NRB, co eliminuje znaczącą klasę potencjalnych ataków.

Wszelkie pytania związane z powyższą informacją oraz wątpliwości co do nietypowego zachowania się systemu bankowości elektronicznej prosimy zgłaszać pod numerem telefonu 509678407.