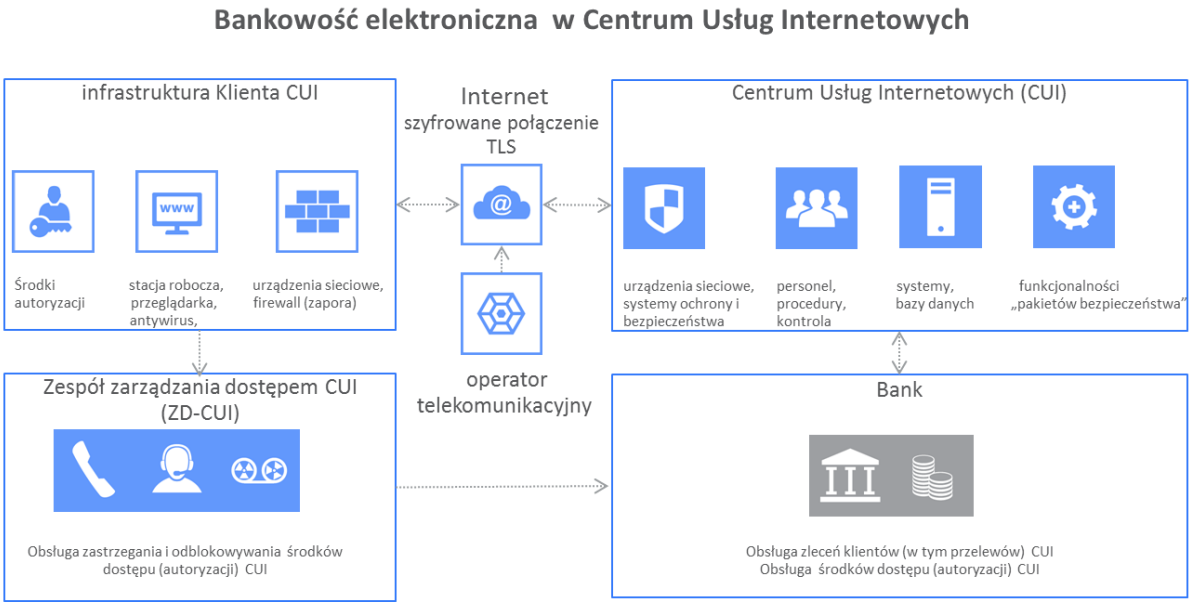
Bank Spółdzielczy w Łańcucie
Rok założenia 1913 Grupa BPS

ZBIÓR DOBRYCH PRAKTYK KORZYSTANIA Z BANKOWOŚCI ELEKTORNICZNEJ

Bankowość elektroniczna w Centrum Usług Internetowych



I. Zasady bezpiecznego korzystania z bankowości elektronicznej

1. Zawsze sprawdzaj na stronie logowania bankowości elektronicznej aktualne zasady bezpiecznego korzystania z bankowości elektronicznej.
2. Szczegółowe informacje o zagrożeniach dla użytkowników bankowości elektronicznej należy weryfikować na stronie Związku Banków Polskich: http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci (link znajduje się na stronie logowania bankowości elektronicznej).
3. Jeśli otrzymasz komunikat o przerwie konserwacyjnej podczas logowania lub realizacji przelewu, koniecznie zrezygnuj z dalszej pracy w bankowości elektronicznej i skontaktuj się z Bankiem.
4. Zabezpiecz komputer aktualnym oprogramowaniem antywirusowym oraz zaporą (firewall).
5. Regularnie aktualizuj system operacyjny, wersję przeglądarki oraz oprogramowanie na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej.
6. Uważaj na nietypowe informacje z banku, nie wykonuj podejrzanych poleceń, a w szczególności nie instaluj oprogramowania z niezaufanego źródła, zarówno na stacji roboczej, przy użyciu której korzystasz z bankowości elektronicznej, jak i w telefonie komórkowym.
7. Po zakończeniu pracy w bankowości elektronicznej wyloguj się używając przeznaczonej do tego opcji w aplikacji, gwarantuje to poprawne zamknięcie sesji przez użytkownika.
8. Nie instaluj oprogramowania, jeżeli instrukcja instalacji zawiera zalecenie rezygnacji ze skanowania aplikacji oprogramowaniem antywirusowym.
9. Chroń dane dostępowe do bankowości elektronicznej.

10. Nie loguj się i nie dokonuj płatności w punktach bezpłatnego publicznego dostępu do Internetu - w tzw. hot-spotach.
11. Zweryfikuj czy certyfikat strony wystawiony jest dla Centrum Usług Internetowych przez firmę Thawte lub DOMENY.PL (kliknięcie na "zatrzaśniętą kłódkę" w pasku przeglądarki). Brak "zatrzaśniętej kłódki" oznacza, że mamy do czynienia z niebezpiecznym połączeniem, w którym dane nie są szyfrowane.
12. Sprawdź poprawność numeru NRB przed i po podpisie przelewu.
13. Zwróć szczególną uwagę na poprawność numeru NRB po wklejeniu go ze schowka systemu. Najlepiej zrezygnuj z kopiowania NRB.
14. Nigdy nie ignoruj ostrzeżeń przeglądarki o błędnym certyfikacie.
15. Weryfikuj numer NRB w otrzymanym SMSie autoryzacyjnym, jeśli jest inny niż oczekiwany, zrezygnuj z autoryzacji przelewu.
16. Jeśli otrzymasz komunikat o przerwie konserwacyjnej podczas realizacji przelewu, zrezygnuj z dalszej realizacji przelewu i skontaktuj się z Bankiem.
17. Ustal limity operacji dla przelewów.

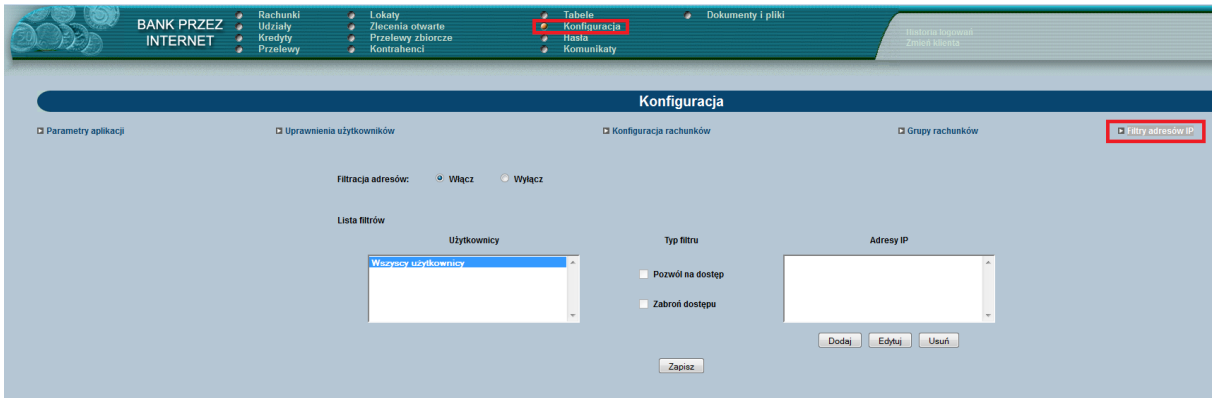
II. Bankowość korporacyjna - funkcjonalności podnoszące odporność systemu przed zaniedbaniami użytkownika.

1. Filtrowanie adresów IP.

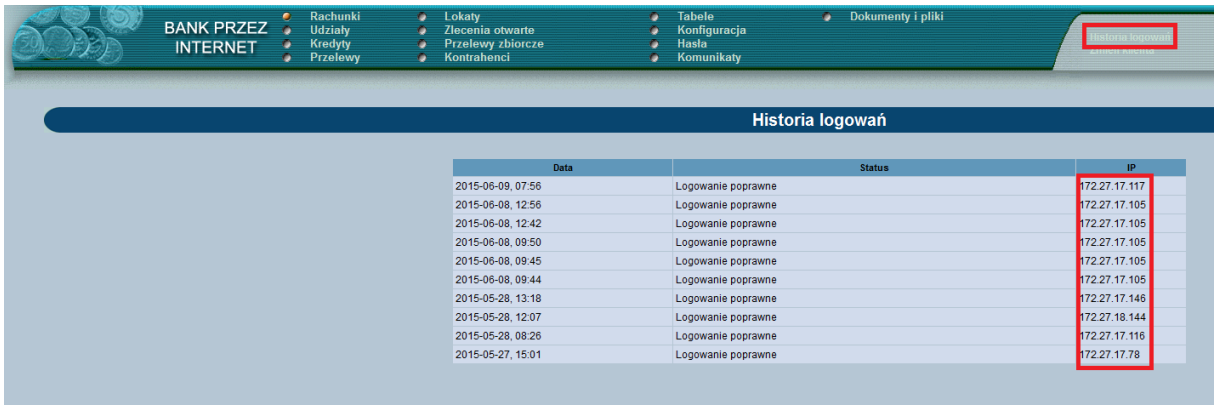
Funkcjonalność <u>wymaga</u> konfiguracji przez użytkownika.

W bankowości korporacyjnej dostępne jest bardzo skuteczne narzędzie dające możliwość określenia, z jakiego adresu internetowego (IP) dozwolone jest logowanie. Funkcjonalność tą przystosowaliśmy również do tzw. dynamicznych IP poprzez możliwość definiowania klasy adresowej np. dostawcy Internetu. Filtry IP można zdefiniować na poziomie Klienta lub poszczególnych użytkowników.

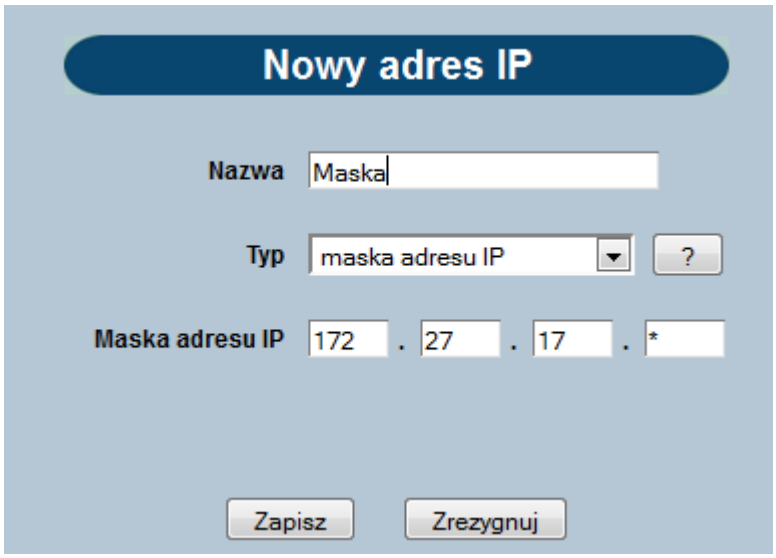
Filtry IP są definiowane w opcji: Konfiguracja -> Filtry adresów IP



Własny adres IP można zweryfikować w opcji: Historia logowań



W przypadku Klientów posiadających tzw. dynamiczne IP, należy na podstawie historii logowań lub po kontakcie z dostawcą Internetu ustalić odpowiednią maskę dla filtru IP. Przykładowo, z zaprezentowanego powyżej zrzutu ekranu wynika, że logowania następują z adresów IP z początkiem '172.27.17' oraz '172.27.18', zatem w takim przypadku należy zdefiniować maski '172.27.17.*' oraz '172.27.18.*'



2. Blokada edycji NRB.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Funkcjonalność zabezpiecza przed podmianą numeru NRB przez osoby nieuprawnione. W przypadku konieczności zmiany przygotowanego przelewu wymagana jest dodatkowa autoryzacja. Nawet osoby, które wykradły login i hasło nie mogą ingerować w NRB na wprowadzanych przelewach.

3. Podpis usuwania zleceń.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Zabezpieczenie chroni przed usunięciem i przygotowaniem na to miejsce „podobnego" (ze zmienionym NRB) przelewu. Wraz z blokadą edycji NRB stanowi skuteczną ochronę przed manipulowaniem NRB, przy założeniu, że osoba podpisująca przelewy weryfikuje ilość podpisywanych przelewów.

4. Autoryzacja dodawania/edycji szablonów/kontrahentów.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Funkcjonalność zabezpiecza przed nieuprawnioną modyfikacją szablonów przelewów oraz kontrahentów. Ingerencja w listę zdefiniowanych szablonów/kontrahentów możliwa jest jedynie po dodatkowej autoryzacji.

5. Logowanie tokenem RSA lub VASCO.

Funkcjonalność wymaga wydania tokena przez Bank dla użytkownika.

Kod na wyświetlaczu tokena (wskazanie) zmienia się w określonych odstępach czasu. Dzięki temu pozyskanie pełnych danych do logowania przez osoby nieuprawnione jest niemożliwe.

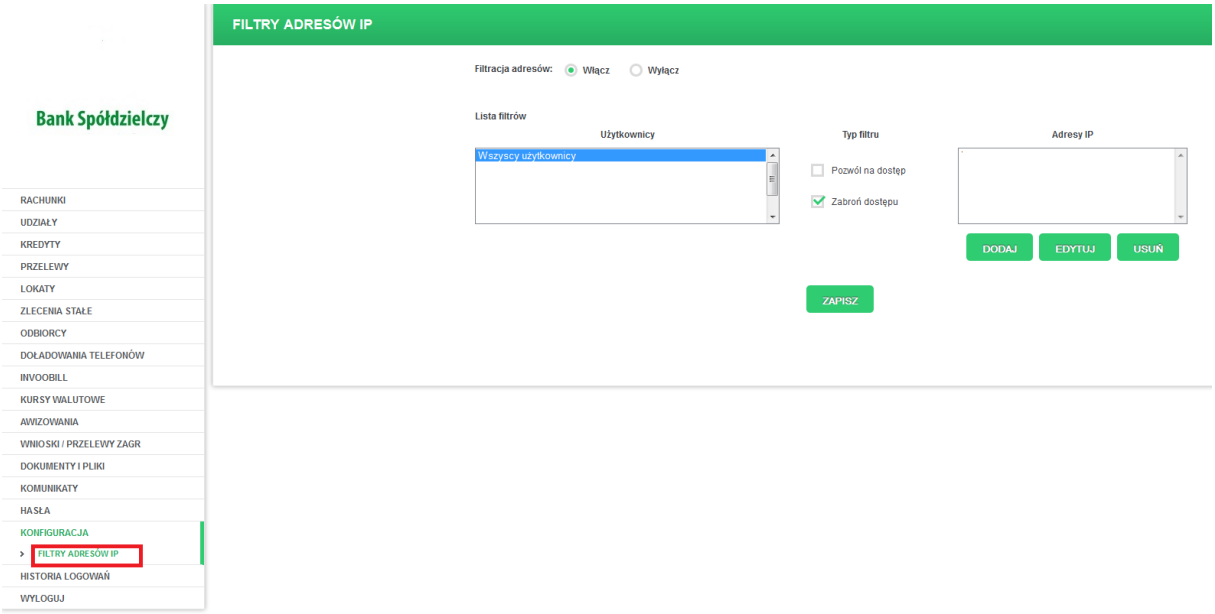
III. Bankowość detaliczna - funkcjonalności podnoszące odporność systemu przed zaniedbaniami użytkownika

1. Filtrowanie adresów IP.

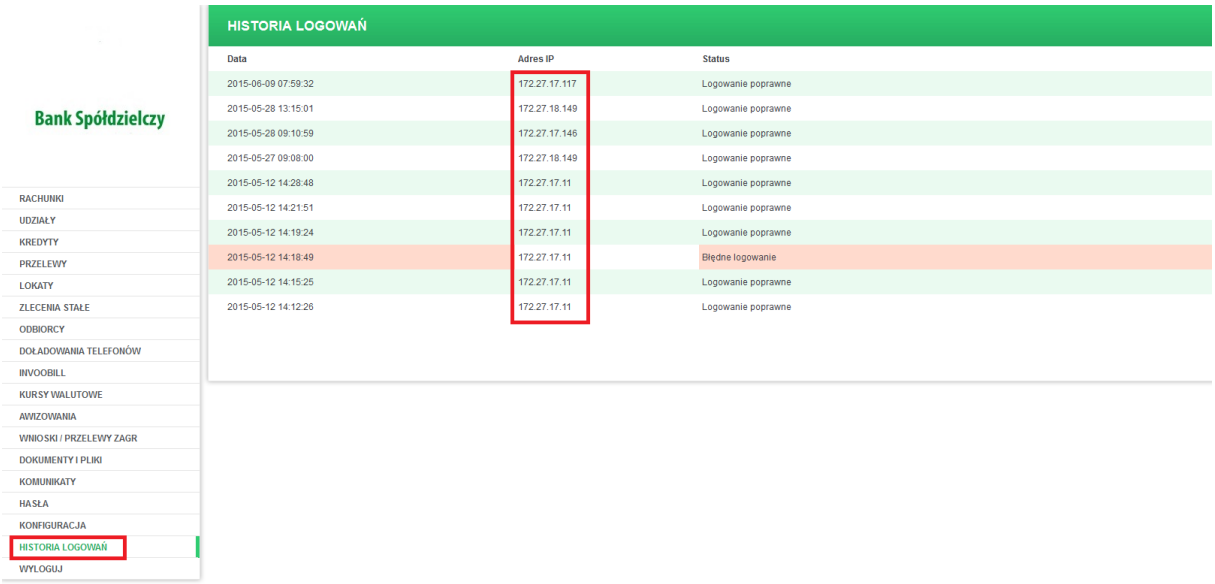
Funkcjonalność wymaga konfiguracji przez użytkownika.

W bankowości detalicznej dostępne jest bardzo skuteczne narzędzie dające możliwość określenia, z jakiego adresu internetowego (IP) dozwolone jest logowanie. Funkcjonalność tą przystosowaliśmy również do tzw. dynamicznych IP poprzez możliwość definiowania klasy adresowej np. dostawcy Internetu. Filtry IP można zdefiniować na poziomie Klienta lub poszczególnych użytkowników.

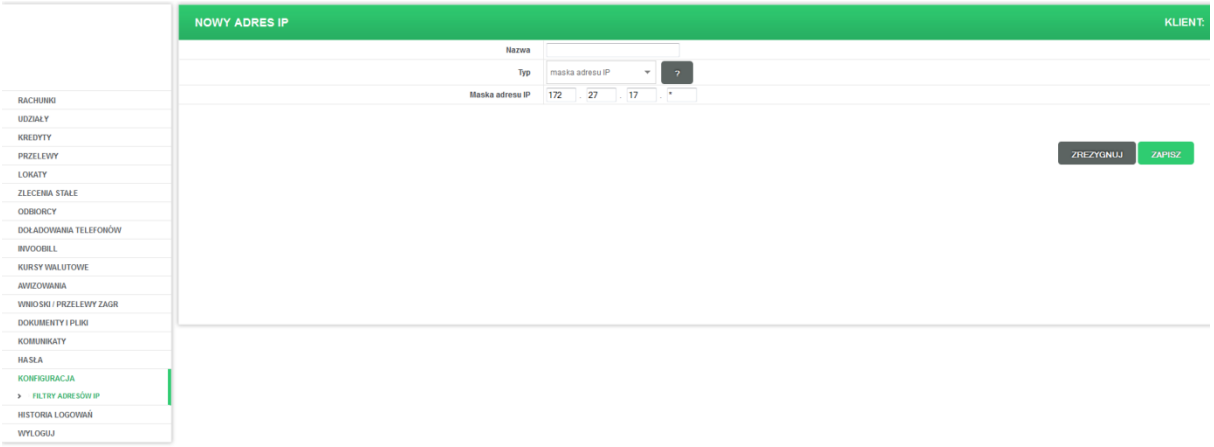
Filtry IP są definiowane w opcji: Konfiguracja -> Filtry adresów IP



Własny adres IP można zweryfikować w opcji: Historia logowań



W przypadku Klientów posiadających tzw. dynamiczne IP należy na podstawie historii logowań lub po kontakcie z dostawcą Internetu ustalić odpowiednią maskę dla filtru IP. Przykładowo z zaprezentowanego powyżej zrzutu ekranu wynika, że logowania następują z adresów IP z początkiem ‘172.27.17’ oraz ‘172.27.18’ zatem w takim przypadku należy zdefiniować dwie maski ‘172.27.17.*’ oraz ‘172.27.18.*’



2. Autoryzacja dodawania/edycji szablonów/odbiorców.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Funkcjonalność zabezpiecza przed nieuprawnioną modyfikacją szablonów przelewów oraz odbiorców. Ingerencja w listę zdefiniowanych szablonów/odbiorców możliwa jest jedynie po dodatkowej autoryzacji.

3. SMS z informacją o zalogowaniu.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Klient otrzymuje SMS z informacją o zalogowaniu do bankowości elektronicznej.

Informacja taka pozwala Klientowi na szybką reakcję w przypadku stwierdzenia nieautoryzowanego dostępu. Klient ma możliwość natychmiastowego zablokowania dostępu do bankowości elektronicznej bezpośrednio w Banku.

4. SMS z informacją o złożonym przelewie.

Funkcjonalność nie wymaga konfiguracji przez użytkownika.

Klient otrzymuje SMS z informacją o złożonym przelewie W przypadku wykrycia nieautoryzowanego przelewu, Klient ma możliwość zablokowania przelewu bezpośrednio w Banku.

IV. Zachowania użytkownika, a ryzyko wykonywania operacji finansowych przez Internet.

Bankowość elektroniczna jest wygodną i bezpieczną formą korzystania z usług bankowych, w tym składania zleceń finansowych. W ostatnim czasie nasiliły się ataki na Klientów bankowości elektronicznej. Przestępcy nie mogąc złamać zabezpieczeń infrastruktury dostawców bankowości elektronicznej (Banków, dostawców technologii i usług), skupili się na łamaniu zabezpieczeń infrastruktury Klientów i bazowaniu na wzorcach ich zachowań. W czasach globalizacji, szalonego rozwoju usług mobilnych, coraz wyższych wymagań użytkowników co do ergonomii łatwo zapomnieć użytkownikowi o przestrzeganiu podstawowych zasad bezpieczeństwa, co przestępcy, stosując coraz bardziej wyrafinowane metody ataku, mogą wykorzystać.

Szanowny użytkowniku, bezwzględnie stosuj się do zasad bezpieczeństwa jakie publikuje Bank, w przeciwnym razie, Twoja twierdza, jaką jest bankowość elektroniczna, ma zostawione otwarte wrota.

Bank ze swojej strony dokłada starań aby nieustannie rozwijać technologie i usługi, które będą wspierać użytkownika w wygodnym i bezpiecznym korzystaniu z bankowości elektronicznej.