Bezpieczeństwo

1. **Bezpieczeństwo aplikacji internetowej TFI PZU S.A.**

W sieci Internet można spotkać się z atakami polegającymi na próbach wyłudzenia danych logowania. Atak polega na uruchomieniu fałszywej strony, która wyglądem imituje oryginalną, lecz w rzeczywistości służy wyłudzeniu danych dostępowych do systemu. Zagrożenie to nazywane jest phishingiem.

- Najbezpieczniejszą metodą w celu zalogowania się do aplikacji internetowej TFI PZU SA jest logowanie się ze strony https://www.pzu.pl.
- Nie należy używać w tym celu odnośników otrzymanych w poczcie elektronicznej lub umieszczonych na innych stronach niż PZU. Może to być próba oszustwa, polegająca na podaniu adresu fałszywej strony w celu przechwycenia informacji umożliwiających zalogowanie w serwisie i zarządzanie kontem.
- TFI PZU SA nigdy nie będzie wysyłać korespondencji elektronicznej z prośbą o podanie haseł dostępowych do serwisu. W przypadku otrzymania takiej wiadomości pocztowej, nie należy na nią odpowiadać nadawcy oraz powiadomić TFI PZU SA wysyłając informację na skrzynkę kontakt@pzu.pl.
- Użytkownik zobowiązany jest do ochrony informacji umożliwiających jego identyfikację w aplikacji internetowej TFI PZU SA, w tym nieudostępniania Loginu, Hasła, kodu PIN osobom nieupoważnionym.
- Hasło/kod PIN powinno być przechowywane w sposób bezpieczny. Jeżeli Użytkownik zapisuje je na urządzeniu elektronicznym, powinno być chronione przed odczytem lub przejęciem na przykład przez zastosowanie rozwiązań kryptograficznych (szyfrowanie). Urządzenie elektroniczne wykorzystywane przez Użytkownika, w tym również mobilne, powinno być zabezpieczone hasłem/pinem oraz systemem ochrony przed złośliwym oprogramowaniem
- PZU nie ponosi odpowiedzialności za skutki udostępnienia przez Użytkownika informacji umożliwiających jego identyfikację w Serwisie osobom nieupoważnionym.
- W przypadku podejrzenia, że Login lub Hasło/kod PIN zostały przejęte przez osoby nieupoważnione, Użytkownik jest zobowiązany do niezwłocznego skontaktowania się z PZU na adres kontakt@pzu.pl w celu blokady konta w Serwisie lub zmiany danych dostępowych.
- Przed każdym logowaniem do aplikacji internetowej należy sprawdzić certyfikat bezpieczeństwa. W obrębie okna przeglądarki powinna znajdować się ikona zamkniętej kłódki - należy na nią kliknąć, po czym otworzy się okno z właściwościami certyfikatu, gdzie należy sprawdzić następujące parametry:

o zakładka "Ogólne" (ang. "General"):

o wystawiony dla: ("Issued to") - prawidłowa informacja to: "*.pzuci.pl"

o wystawiony przez: ("Issued by") - aktualny certyfikat wystawiony jest przez " Certum Organization Validation CA SHA2 "

o data ważności certyfikatu ("Valid from ... to ...") - prawidłowa informacja to: Ważny od 2017-06-14 do 2019-06-14

- zakładka "Szczegóły" (ang. "Details") tzw. odcisk palca ("Thumbprint") - prawidłowa wartość tego pola to: 2f 60 90 63 1f dc 29 1f 28 8d 7e aa 3d 04 90 ae 9e 18 35 c4
- zakładka "Ścieżka certyfikacji" (ang. "Certification path") - prawidłowa ścieżka zawiera trzy elementy: " Certum Trusted Network CA / Certum Organization Validation CA SHA2 /*.pzuci.pl"

o Połączenie z aplikacją internetową TFI PZU S.A. jest szyfrowane przy użyciu protokołu internetowego SSL (Secure Socket Layer) z 2048 bitowym kluczem szyfrującym. Taki system wymiany danych między Uczestnikiem a Funduszami umożliwia osiągnięcie wysokiego poziomu bezpieczeństwa. Dodatkowo stosowanymi zabezpieczeniami są:

- blokowanie kodu PIN po trzech nieudanych próbach logowania,
- automatyczne wylogowanie po piętnastominutowej bezczynności ze strony Uczestnika.

Zalecane jest używanie przeglądarki internetowej, która umożliwia szyfrowanie z siłą 2048 bitów, takiej jak np. MS Internet Explorer w wersji 11 i nowszej lub Mozilla Firefox w wersji 3.0 i nowszej. Do prawidłowego działania aplikacji wymagane jest włączenie obsługi Javascript oraz zezwolenie na zapisywanie plików cookie w ustawieniach przeglądarki internetowej.

Informacja o zagrożeniach wynikających ze świadczenia usług drogą elektroniczną / elektronicznych kanałów dostępu

Elektroniczny kanał dostępu – oznacza udostępniane przez TFI PZU SA systemy teleinformatyczne i rozwiązania techniczne, opisanych w niniejszych Zasadach, które umożliwiają korzystanie z usług świadczonych drogą elektroniczną, w tym składanie przez Usługobiorcy dyspozycji dotyczących Funduszu i Jednostek Uczestnictwa za pomocą urządzeń operujących w sieci Internet lub telefonicznej;

Podstawowe zagrożenia związane z korzystaniem z usług w sieci Internet – w tym usług oferowanych przez TFI PZU SA w ramach elektronicznych kanałów dostępu – to:

o podszywanie się w celu wyłudzenia informacji,
o działanie złośliwego oprogramowania,
o niechciana poczta - spam.

Zagrożenia dotyczą nie tylko komputerów, ale też innego sprzętu przenośnego, np. smartfonów, tabletów.

Phishing - to wyłudzanie danych umożliwiających dostęp do danej usługi (loginu, hasła, PIN), numerów kart kredytowych itp. Najczęściej są to fałszywe powiadomienia imitujące komunikaty z instytucji rozsyłane drogą elektroniczną, w których nakłania się użytkowników do zalogowania na spreparowane strony internetowe naśladujące oryginalne. Celem jest przechwycenie danych dostępowych.

Złośliwe oprogramowanie – takie programy, które są wykorzystywane w celach przestępczych lub mają na

celu wyrządzenie szkody użytkownikowi. Należą do nich m.in. wirusy komputerowe i oprogramowanie szpiegujące.

- **Wirus komputerowy** to oprogramowanie złośliwe, które przenosi się poprzez zapis zainfekowanego pliku na nośniku danych np. dysku twardym, pendrive. Celem wirusa jest kradzież lub usunięcie danych, zakłócenie pracy urządzenia lub przejęcie kontroli nad komputerem. Najczęściej do zarażenia wirusem elektronicznym dochodzi po pobieraniu plików z niezaufanego źródła internetowego lub otwarciu załącznika w poczcie elektronicznej.
- **Program szpiegujący** – to taki, który w sposób ukryty monitoruje i przesyła dane o użytkowniku do przestępcy. Może gromadzić i przekazywać zarówno dane umieszczone na urządzeniu jaki i śledzić nasze działania np. ruchy myszką, tekst wpisywany z klawiatury.

Niechciana poczta lub spam to niezamawiane lub niepotrzebne wiadomości elektroniczne rozsyłane jednocześnie do wielu odbiorców. Często przenoszą wirusy komputerowe, oprogramowanie szpiegujące, odnośniki do złośliwych lub fałszywych stron.

- **Podstawowe zasady bezpieczeństwa**

9. Każdy użytkownik serwisu powinien dbać o bezpieczeństwo swoich urządzeń, które służą dostępowi do sieci Internet. Takie urządzenie powinno posiadać program antywirusowy z aktualną bazą definicji wirusów, aktualną i bezpieczną wersję przeglądarki internetowej oraz włączoną zaporę sieciową (ang. firewall). Użytkownik powinien ponadto cyklicznie sprawdzać, czy system operacyjny i programy zainstalowane na nim posiadają najnowsze aktualizacje, ponieważ w atakach wykorzystywane są błędy wykryte w zainstalowanym oprogramowaniu. Producenci programów starają się eliminować takie zagrożenia za pomocą aktualizacji.
10. Dane dostępowe do usług oferowanych w sieci Internet – np. loginy, hasła, PIN, certyfikaty elektroniczne itp.,– powinny być zabezpieczone. Nie należy ich ujawniać lub przechowywać na urządzeniu w formie, która umożliwia nieautoryzowany dostęp i odczyt.
11. Zaleca się ostrożność podczas otwierania załączników lub klikania odnośników w wiadomościach, których się nie spodziewaliśmy np. od nieznanych nadawców. W przypadku jakichkolwiek wątpliwości warto się skontaktować z nadawcą np. telefonicznie.
12. Zaleca się uruchomienie w przeglądarce internetowej filtrów antyphishingowych czyli narzędzi, które sprawdzają, czy wyświetlona strona internetowa jest autentyczna i nie służy wyłudzaniu informacji, np. poprzez podszywanie się pod osobę lub instytucję.
13. Pliki powinny być pobierane tylko z zaufanych miejsc. Nie zalecamy instalowania oprogramowania z niezweryfikowanych źródeł. Dotyczy to również urządzeń przenośnych, np. smartfonów, tabletów.
14. Podczas używania domowej sieci bezprzewodowej (Wi-Fi) należy ustalić bezpieczne i trudne do złamania hasło dostępu do sieci. Rekomenduje się także korzystanie najwyższych możliwych standardów szyfrowania sieci bezprzewodowych Wi-Fi, które są możliwe do uruchomienia na posiadanym sprzęcie np. WPA2.