BEZPIECZEŃSTWO APLIKACJI INTERNETOWEJ

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.

1. Najbezpieczniejszą metodą w celu zalogowania się do aplikacji internetowej jest logowanie się ze strony https://www.pzu.pl.
2. 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.
3. PZU 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 PZU wysyłając informację na skrzynkę kontakt@pzu.pl.
4. Hasło jest informacją poufną i nie należy go ujawniać osobom trzecim.
5. 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:
   a) w zakładce „Ogólne" (ang. "General"):
      - dla kogo został wystawiony certyfikat ("Issued to") – prawidłowa informacja to: "secure.pzuci.pl",
      - wystawca certyfikatu ("Issued by") – aktualny certyfikat wystawiony jest przez "Thawte SSL CA,
      - data ważności certyfikatu ("Valid from ... to ...") – prawidłowa informacja to: Ważny od ,,2015-06-05 do 2017-07-05",
   b) w zakładce „Szczegóły" (ang. "Details") tzw. odcisk palca ("Thumbprint") – prawidłowa wartość tego pola to: 68 2E 1C 85 1A F2 DD 99 4F 17 06 70 4F 7D 7E 97 5D 26 F4 48,
   c) „Ścieżkę certyfikacji" (ang. "Certification path") – prawidłowa ścieżka zawiera trzy elementy: "thawte/Thawte SSL CA/secure.pzuci.pl".
6. Połączenie z serwisem jest szyfrowane przy użyciu protokołu internetowego TLS/SSL. Taki system wymiany danych umożliwia osiągnięcie wysokiego poziomu bezpieczeństwa.
7. Dodatkowo stosowanymi zabezpieczeniami są:
   a) blokowanie kodu PIN/hasła po trzech nieudanych próbach logowania,
   b) automatyczne blokowanie po piętnastominutowej bezczynności ze strony Użytkownika.
8. Zalecane jest używanie przeglądarki internetowej, która umożliwia szyfrowanie SSL z siłą 2048 bitów, takiej jak np. MS Internet Explorer w wersji 11.0 i nowszej lub Mozilla Firefox 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

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

a) podszywanie się w celu wyłudzenia informacji,
b) działanie złośliwego oprogramowania,
c) 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.

1. **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.
2. **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

1. 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.
2. 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.
3. 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.
4. 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.
5. Pliki powinny być pobierane tylko z zaufanych miejsc. Nie zalecamy instalowania oprogramowania z niezweryfikowanych źródeł. Dotyczy to również urządzeń przenośnych, np. smartfonów, tabletów.
6. 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.