Wytyczne dla użytkowników w zakresie ochrony danych dostępowych do przekazania kierownikom jednostek eksploatujących systemy.
(2018.02.19)

Tło.
W ogólnouczelnianych systemach informatycznych PŁ użytkownicy uwierzytelniają się za pomocą poświadczeń:
- UID (user identificator) – jawny identyfikator użytkownika,
- PASSWORD – tajne hasło.
Kształt tych poświadczeń jest regulowana zarządzeniem rektora nr 15/2010. Uzyskanie początkowych poświadczeń jest możliwe po nawiązaniu stosunku prawnego z uczelnią (umowa o pracę lub cywilno-prawna w przypadku pracownika, zrekrutowanie na studia w przypadku studenta) oraz po wizycie w odpowiednim BOK (biurze obsługi klienta), gdzie następuje identyfikacja użytkownika i wydanie hasła początkowego.
Obok zdecydowanej większości systemów, w których uwierzytelnianie wymaga UID/PASSWORD, występują w zbiorze systemów ogólnouczelnianych takie, które wymagają innego rodzaju poświadczenia w postaci certyfikatu cyfrowego X509. Takimi systemami są SID, Eduroam, OpenVPN. Każdy użytkownik PŁ może uzyskać certyfikat za pośrednictwem portalu WWW. W portalu należy się zalogować za pomocą atrybutów UID/PASSWORD, następnie po wybraniu odpowiednich opcji wygenerować klucze RSA i uzyskać certyfikat X509. Generacja kluczy następuje w przeglądarce użytkownika (lokalnie), dzięki czemu klucz prywatny RSA nie opuszcza komputera użytkownika. W wyniku operacji użytkownik zapisuje na swoim dysku lokalnym tzw. magazyn kluczy PKCS12, który zawiera klucz prywatny RSA, certyfikat X509 użytkownika oraz certyfikat X509 instytucji poświadczającej, w tym przypadku PŁ. Od tej pory użytkownik używa pary atrybutów (klucz prywatny RSA i certyfikat X509) do uwierzytelniania w wymienionych trzech systemach oraz opcjonalnie może ich używać do operacji dodatkowych takich jak składanie podpisu cyfrowego lub szyfrowanie treści.
Certyfikat jest zdecydowanie mocniejszym, a zatem bezpieczniejszym, rodzajem poświadczenia, niż UID/PASSWORD, ponieważ klucze szyfrujące stanowią długi ciąg znaków/cyfr, niemożliwy do zapamiętania przez człowieka, po przeczytaniu lub usłyszeniu. Dzięki temu obca osoba nie może przejąć tego identyfikatora metodami socjotechnicznymi. Do przejęcia koniecznym jest fizyczne skopiowanie identyfikatora na nośnik danych.

Zalecenia dla użytkowników
Atrybuty uwierzytelniana stanowią element tożsamości użytkownika, a ich przejęcie przez inne osoby może powodować poważne konsekwencje od finansowych po karne. Dlatego w interesie, zarówno PŁ, jak i każdego użytkownika jest ochrona własnych atrybutów uwierzytelniania.
Atrybuty uwierzytelniania są zagrożone następującymi czynnikami kompromitacji:

1. Metody socjotechniczne.
   Przejęcie atrybutu uwierzytelniania przez osoby nieuprawnione następuj w wyniku niefrasobliwego zachowania użytkownika (zapisywanie hasła na kartkach, podawanie hasła innym osobom, nawet zaufanym, konstruowanie schematycznych haseł zawierających imiona bliskich, daty urodzin, tablic rejestracyjnych), multiplikowanie magazynu PKCS12 i kopiowanie na zewnętrzne nośniki danych.
   Ponadto nie należy zbyt szeroko stosować hasła w innych systemach, administrowanych poza PŁ.
2. Metody algorytmiczne.
   Atrybuty uwierzytelniania mogą zostać złamane metodami algorytmicznymi. Problem ten dotyczy głównie haseł. Hasła mogą być łamane metodą generowania kolejnych permutacji, aż do uzyskania prawidłowego wzorca. Z uwagi na długość klucza RSA, znacznie większą niż długość hasła problem ten w stopniu znikomym dotyczy kluczy/certyfikatów. Aby wzmocnić odporność haseł na łamanie algorytmiczne, należy wydłużać hasła i często je

zmieniać. A jeszcze lepiej, zamiast „userId/password”, używać poświadczeń opartych o klucze asymetryczne RSA.

3. Metody mistyfikacyjne („fishing”).
   Polegają na tym, że atakujący podszywa się pod zaufany serwis, podstawiając fałszywy serwis podobny w wyglądzie i nazwie, gdzie użytkownik próbuje zidentyfikować się w typowy sposób poprzez podanie identyfikatora i hasła. Jednak nie dochodzi do zalogowania, tylko następuje komunikat o błędzie, po czym użytkownik jest przekierowywany do prawdziwego serwisu. W momencie niby błędnego logowania zostają przechwycone poświadczenia, a użytkownik myśli, że popełnił błąd przy wpisywaniu hasła. Po przekierowaniu do właściwego serwisu, ponowna próba logowania kończy się sukcesem, co prawdopodobnie niweluje ewentualne podejrzenia. Sposobami nakierowania na użytkownika na fałszywy serwis może być podesłanie na e-mail linku lub utworzenie w DNS serii nazw domenowych różniących się bardzo nieznacznie od nazwy atakowanego serwisu, np. jedną literą, a pomyłki literowe często się zdarzają przy wpisywaniu nazw w oknie adresowym przeglądarki WWW. Należy zatem ostrożnie korzystać z podsyłanych linków, sprawdzać nazwy i sprawdzać wystawców certyfikatów poświadczających strony WWW.
   Ponadto dobrą praktyką jest zapamiętywanie linków do używanych serwisów w zakładkach przeglądarki (np. „ulubione”) oraz zapamiętywaniu poświadczeń w magazynie haseł przeglądarki (opcja „zapamiętaj mnie”). Stosując jednak praktykę zapamiętywania poświadczeń, należy mieć na uwadze aby nie pozostawiać poza kontrolą niezabezpieczonego komputera osobistego, ponieważ wówczas ktoś postronny mógłby się dostać na nasze konto bez znajomości hasła. Zawsze oddalając się od komputera, z tego i innych względów, należy komputer osobisty zabezpieczyć (wylogować się, zablokować, uśpić lub wyłączyć).
4. Metody hackerskie.
   Polegają na zainfekowaniu naszego komputera różnymi formami wirusów (malware, trojan, worm, itp.), które w sposób niewidoczny dla użytkownika mogą przechwycić poświadczenia i wysłać je do atakującego. W ten sposób mogą zostać przejęte również inne dane zapisane na naszym komputerze.
   Dlatego należy dbać o zabezpieczenia stacji roboczej poprzez stałą aktualizację systemu operacyjnego i programów (wg harmonogramu producentów), a także stosować zabezpieczenia antywirusowe. Należy również unikać podłączania zewnętrznych nośników danych, jeżeli nie pochodzą z zaufanego źródła, uruchamiania załączników przysłanych pocztą elektroniczną, jeżeli pochodzą od nieznanych nadawców, nie wchodzić na strony internetowe o podejrzanej lub nieznanej reputacji, reagować asertywnie na ostrzeżenia podawane przez przeglądarkę WWW, program antywirusowy lub system operacyjny.