Zalecenia dotyczące bezpieczeństwa logowania

Logowanie do usługi korzystającej z uwierzytelniania federacyjnego zazwyczaj przebiega według następującego scenariusza:

1. Użytkownik wybiera z listy swoją instytucję macierzystą (PCz)
2. Strona usługi dokonuje przekierowania na stronę Centralnego Punktu Logowania PCz
3. Użytkownik loguje się w Centralnym Punkcie Logowania PCz
4. Centralny Punkt Logowania PCz pokazuje pytanie o zgodę na przekazanie do Usługi wymaganych przez nią atrybutów.
5. Jeżeli użytkownik wyrazi zgodę, to jest przekierowywany na stronę Usługi i jest zalogowany, jeżeli zgody nie wyrazi, to zalogowanie nie dochodzi do skutku.

Jeżeli użytkownik był już wcześniej zalogowany w Centralnym Punkcie Logowania PCz, to punkty 2 i 3 wykonają się automatycznie.

Użytkownik powinien zawsze potwierdzać autentyczność strony Centralnego Punktu Logowania PCz poprzez sprawdzenie, że adres pokazany w przeglądarce zaczyna się od https://logowanie.man.pcz.pl, a przeglądarka pokazuje symbol bezpiecznego połączenia. Gdyby adres strony był inny, to oznacza to próbę fałszerstwa i pod żadnym pozorem do takiej strony nie należy się logować, a całą sprawę zgłosić administratorom PCz.

Korzystanie z zewnętrznych usług, które wywołują stronę logowania PCz jest obarczone potencjalnym zagrożeniem. Fałszywa usługa może przekierować użytkownika na podrobioną stronę logowania i w ten sposób wyłudzić jego identyfikator i hasło.

Sposobem gwarantującym wysokie bezpieczeństwo jest wstępne zalogowanie na stronie Centralnego Punktu Logowania PCz. Do czasu wylogowania lub zamknięcia przeglądarki użytkownik powinien być automatycznie wpuszczany do wszystkich dostępnych dla niego usług. W takiej sytuacji pojawienie się strony logowania powinno być potraktowane jako sygnał alarmowy. Usługa może zażądać ponownego zalogowania, ale jest to nietypowe. Niezbędne jest zatem sprawdzenie autentyczności strony logowania.