Dziura w szwajcarskim systemie wyborczym

14 marca 2019

W kodzie źródłowym szwajcarskiego systemu wyborczego znaleziono poważny błąd kryptograficzny. Umożliwia on osobom z wewnątrz, które zarządzają tym systemem lub go implementują, na manipulowanie głosami.

Specjaliści z Uniwersytetu w Melbourne, kanadyjskiego Open Privacy Research Society oraz belgijskiego Uniwersytetu Katolickiego w Louvain-la-Neuve przeanalizowali upubliczniony kod systemu wyborczego i znaleźli w nim błąd.

W systemie, którym zarządza SwissPost, szyfrowane głosy muszą zostać przetasowane, by chronić prywatność wyborcy. Zarządzający przetasowaniem muszą dostarczyć matematycznego dowodu, że podczas przetasowania głosy nie uległy zmianie. Dopiero dzięki temu można zweryfikować poprawność głosowania.

Eksperci znaleźli jednak w algorytmie lukę, która pozwala na zmianę głosów i wygenerowanie kodu dowodzącego, że nie zostały one zmienione.

„Nic w naszej analizie nie wskazuje, by luka taka została celowo wprowadzona, jednak jej istnienie nas martwi i budzi poważne pytania o jakość pozostałej części kodu" – mówi Sarah Jamie Lewis z Kanady.

„W tym przypadku analizy wskazują, że mamy tutaj do czynienia z naiwną implementacją złożonego protokołu kryptograficznego przez osoby, które działały w dobrej wierze, ale brak im było pełnej wiedzy na temat bezpieczeństwa" – wyjaśnia profesor Vanessa Teague z Melbourne. „Oczywiście, gdyby ktoś chciał wprowadzić taki kod, by móc manipulować wynikami wyborów, zrobiłby to w taki sposób, by wyglądało to na przypadek. Jednak nie mamy żadnych dowodów, by stwierdzić, że tak właśnie

było” – dodaje uczona.

Autorstwo: Mariusz Błoński
Na podstawie: TechXplore.com
Źródło: KopalniaWiedzy.pl