Warszawa, 30 marca 2016 roku

Szanowna Pani,
Anna Streżyńska
Minister Cyfryzacji

Wnioskodawca:
Karol Breguła
ul. {…}
{…}

Petycja o uwzględnienie dwuskładnikowej autoryzacji

Szanowna Pani Minister,

Kierujemy do Pani niniejszą petycję stosownie do treści artykułu 63 Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., który przesądza, że możliwość zgłaszania petycji, skarg i wniosków do organów administracji publicznej stanowi konstytucyjne prawo obywatela.

Uwzględniając również art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (t.j. Dz. U. z 2015 r. poz. 2135 z późn. zm.), który przesądza, że minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia m. in. podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną.

Wnosimy w interesie publicznym o podjęcie działań na rzecz zmian w przepisach rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Uważamy, że **przepisy powinny przewidywać możliwości autoryzacji wieloskładnikowej zamiast wymogu ciągłej zmiany haseł, albo że wymóg zmiany haseł powinien zostać ograniczony w przypadku wprowadzenia takiej formy autoryzacji.**

Uważamy również, że winna zostać zachowana dopuszczalność autoryzacji samym hasłem na dotychczasowych zasadach. Jednak należy wprowadzić nowe rozwiązania w sytuacji decyzji administratora o wykorzystaniu autoryzacji wieloskładnikowej.

W dotychczasowych przepisach wskazano, że jeśli do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. W poszczególnych przypadkach określono wymogi co do złożoności haseł.

Metody uwierzytelniania można podzielić na wykorzystujące:

- coś co wiesz (*something you know*) – informacja będąca w wyłącznym posiadaniu

uprawnionego podmiotu, na przykład hasło lub klucz prywatny;

- coś co masz (*something you have*) – przedmiot będący w posiadaniu uprawnionego podmiotu, na przykład generator kodów elektronicznych (token), telefon komórkowy (kody SMS, połączenie autoryzacyjne) lub klucz analogowy,
- coś czym jesteś (*something you are*) – metody biometryczne.

W nowoczesnych systemach komputerowych przed uzyskaniem dostępu często stosuje się jednak uwierzytelniani wieloskładnikowe (*multi-factor authentication*), w szczególności dwuskładnikowe (*two-factor authentication*), czyli łączące dwie różne metody uwierzytelniania.

Jest to praktykowane, ponieważ w komunikacji elektronicznej stosowanie samego hasła wiąże się z różnego rodzaju ryzykiem, a wykorzystanie kilku form uwierzytelnienia może ograniczać skutki przechwycenia (*keylogger*), albo podsłuchania (*sniffer*) hasła po którym przestaje ono być wówczas znane wyłącznie osobie uprawnionej, zaś kradzież może pozostać niezauważona. Ryzyko to można ograniczyć, wprowadzając dodatkowy składnik uwierzytelniania wykorzystując kilka form autoryzacji jednocześnie np.:

- token istniejący w jednym, unikatowym egzemplarzu, więc jego użycie wymaga fizycznego dostępu lub kradzieży, która zostanie zauważona (cecha coś co masz);
- użycie tokenu wymaga dodatkowo podania hasła (np. w postaci kodu PIN), więc bez jego znajomości token będzie nieprzydatny, nawet w razie kradzieży (cecha coś co wiesz).

Uwierzytelnienie dwuskładnikowe stosuje większość banków internetowych, usługa poczty Gmail, Facebook, Apple, platformy gier (Battle.net) i wiele innych. Powszechnie dostępne są interfejsy programistyczne do jednorazowych haseł przesyłanych za pomocą SMS, tokeny sprzętowe, jak i programowe generatory haseł TOTP (*Time-based One-Time Password Algorithm*) np. Google Authenticator.

Warto zwrócić uwagę, że standardy regulacyjne dotyczące dostępu do systemów rządu federalnego USA wymagają nawet używania uwierzytelniania wieloskładnikowego, aby uzyskać dostęp do krytycznych zasobów IT, na przykład podczas logowania do urządzeń sieciowych podczas wykonywania zadań administracyjnych oraz przy dostępie do uprzywilejowanego konta. Również publikacja „The Critical Security Controls for Effective Cyber Defense”, wydana przez instytut SANS, przygotowana przez rządowe agencje i komercyjnych ekspertów śledczych i d/s bezpieczeństwa stanowczo zaleca wykorzystanie takich rozwiązań[1].

Tymczasem obowiązujące przepisy o ochronie danych osobowych wydają się nieadekwatne do rzeczywistości nie uwzględniając w/w możliwości. W miejsce tego wymagają autoryzacji hasłem, które musi ulegać częstej zmianie. Taka sytuacja prowadzi wręcz do ograniczenia poziomu bezpieczeństwa, a nie poprawy.

Wymuszona zmiana hasła powstrzymuje dostęp intruzów do konta. W przeciwnym razie mogą oni nadal wykorzystywać zdobyte hasło.

1 CIS Controls for Effective Cyber Defense Version 6.0, SANS Institute, https://www.cisecurity.org/critical-controls.cfm [dostęp 16 marca 2016 roku]

Jednak nie można nie dostrzec, że takie podejście rodzi kilka zasadniczych problemów. Nie wszyscy posiadają zdolność zapamiętania złożonych haseł, co prowadzi do ponownego używania haseł w wielu miejscach lub stosowania haseł schematycznych z wykorzystaniem prostych transformacji. W takim wypadku zbyt skomplikowane i często zmieniane hasła prowadzą do zapisywania ich w jawnej formie, co może narażać na ich kradzież.

Odnośnie schematycznych haseł warto w tym miejscu dostrzec uwagi Lorrie Cranor z amerykańskiej Federalnej Komisji Handlu (FTC), która opisała na stronie FTC badania przeprowadzone na University of North Carolina (w Chapel Hill). Badacze pozyskali ponad 51 tys. hashy haseł do 10 tys. nieaktywnych kont studentów i pracowników, na których wymuszano zmianę hasła co 3 miesiące. Po ich analizie stwierdzono, że dla 17% kont znajomość poprzedniego hasła pozwalała na zgadnięcie kolejnego hasła w mniej niż 5 próbach[2].

Podobne wątpliwości co do skuteczności polityki zmiany haseł wyrażono w badaniach tego problemu przeprowadzonych na Carleton University[3]. Dostrzeżono w nich, że w przypadku wielu ataków jednorazowy dostęp do systemu umożliwia natychmiastowe pozyskanie plików docelowych, założenie tylnych drzwi, zainstalowanie oprogramowania typu keylogger lub innego trwałego, złośliwego oprogramowania, które późniejsze zmiany hasła uczyni nieskutecznymi. Autorzy nawet stawiają tezę, że prawdziwe korzyści z wymuszania zmiany haseł nie rekompensują związanych z tym uciążliwości.

Na podstawie art. 4 ust. 3 ustawy o petycjach wyrażam zgodę na opublikowanie moich danych osobowych w zakresie wyznaczonym przez art. 8 ust. 1 ustawy o petycjach.

Mając na względzie powyższe, niniejsza petycja jest uzasadniona, a jako taka zasługuje na niezwłoczne pozytywne uwzględnienie.

Karol Breguła
[podpis elektroniczny]

Do wiadomości:

- Generalny Inspektor Ochrony Danych Osobowych

2 Lorrie Cranor, Time to rethink mandatory password changes, 2 marca 2016 roku, Federalna Komisja Handlu, ftc.gov, https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes [dostęp 16 marca 2016 roku]; Brian Barrett, Want Safer Passwords? Don’t Change Them So Often, Wired.com 3.10.2016, http://www.wired.com/2016/03/want-safer-passwords-dont-change-often/ [dostęp 16 marca 2016 roku]

3 Sonia Chiasson, P. C. van Oorschot, Quantifying the security advantage of password expiration policies, Designs, Codes and Cryptography, 2015, Volume: 77, Issue 2-3, 401-4