Przemysław Jatkiewicz

Wydział Zarządzania
Uniwersytet Gdański

Metody autoryzacji w systemach informatycznych jednostek samorządowych

1. Wstęp

Dane niezbędne w procesie logowania do systemów informatycznych to bardzo częsty cel nieuprawnionych ataków, o których donoszą media. Hasła użytkowników w każdym opracowanym zgodnie z powszechnie przyjętymi zasadami systemie są przechowywane w formie zaszyfrowanej. Nie przeszkadza to hakerom w podejmowaniu udanych prób ich pozyskania i odszyfrowania. Stąd też można natknąć się w sieci na liczne zestawienia i rankingi najbardziej popularnych wśród użytkowników haseł[1]. Upowszechniająca się opinia, iż hasła są „martwe", znajduje potwierdzenie w fakcie rosnących możliwości technicznych dekryptażu. Na konferencji Passwords^12 zaprezentowano urządzenie, które potrafi sprawdzić 348 mld skrótów haseł na sekundę, szyfrowanych jednym z najbardziej popularnych algorytmów używanych w systemach Windows[2].

Wielkie firmy informatyczne, takie jak Dropbox, Facebook, Microsoft, Google czy Apple, udostępniły w swoich produktach możliwość autoryzacji wieloskładnikowej[3]. Jedynie nieliczni naukowcy podjęli badania dotyczące zasadności dalszego wykorzystania haseł. Wśród nich znaleźli się C. Herley i P.C. van Oorschot, którzy w swej publikacji wykazali, że całkowite wyeliminowanie haseł nie jest możliwe. Alternatywne metody autoryzacji nie spełniają wszystkich wymagań użytkowników, a twierdzenie, iż hasła są „martwe", uznali za przedwczesne oraz szkodliwe, gdyż prowadzą do zaniechania dalszych prac badawczych[4].

---

1 A. Vance, *If your password is 123456, just make it hackme*, „The New York Times" 2010, no. 20.

2 J. Gosney, *Password Cracking HPC*, Passwords^12 Conference, Oslo 2012.

3 A. Dmitrienko, C. Liebchen, C. Rossow, A.R. Sadeghi, *On the (in) security of mobile two-factor authentication*, Technical Report TUD-CS-2014-0029, 2014.

4 C. Herley, P. Van Oorschot, *A research agenda acknowledging the persistence of passwords,* „Security & Privacy IEEE" 2012, vol. 10(1), s. 28–36.

Zdecydowana większość informacji o nieuprawnionym pozyskaniu haseł dotyczy portali internetowych, co nie pozwala na bezpośrednie odniesienie ich do systemów eksploatowanych przez instytucje publiczne. Organizacje rządowe i samorządowe podlegają regulacjom prawnym nakazującym im wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnym z normą ISO 27001[5].

Każda z instytucji jest zobligowana do opracowania i ustanowienia polityki bezpieczeństwa informacji, która m.in. musi zawierać zasady autoryzacji[6]. Nad przestrzeganiem jej zapisów czuwa powołany w tym celu administrator bezpieczeństwa informacji. Do jego obowiązków oprócz monitorowania zabezpieczeń należy także szkolenie użytkowników systemów informatycznych[7].

Przy uwzględnieniu licznych, potwierdzonych relacji prasowych o kradzieży haseł użytkowników systemów biznesowych, jak również prawnych restrykcji odnoszących się do systemów informatycznych instytucji zasadne jest podjęcie badań dotyczących procesu autoryzacji w jednostkach samorządowych, które są najbardziej liczną grupą organizacji publicznych przetwarzających szerokie spektrum informacji o obywatelach.

2. Metodyka badań

Celem przedstawionych badań była identyfikacja uwarunkowań procesu autoryzacji w systemach informatycznych eksploatowanych przez jednostki samorządu terytorialnego. Na ich podstawie wnioskowano o możliwości zastosowania alternatywnych w stosunku do haseł metod logowania. Zastosowano następujące metody badawcze[8]:

- eksperyment;
- ankietowanie;
- wywiad.

Eksperyment polegał na wdrożeniu w jednej z organizacji zasad bezpiecznej autoryzacji w systemie informatycznym na podstawie usług katalogowych[9]. Zasady te były implementowane stopniowo. Po każdym etapie następowała kontrola jakości haseł przez

---

[5] J. Sobczak, *Prawne uregulowania obowiązujące przedsiębiorstwa w zakresie bezpieczeństwa informacji oraz skutki ich naruszenia*, „Zeszyty Naukowe Uczelni Vistula" 2014, nr 35, s. 99–114.

[6] A. Calder, *Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide*, Van Haren Publishing, Zalthommel 2006.

[7] T. Mikkonen, *Perceptions of controllers on EU data protection reform: A Finnish perspective*, „Computer Law & Security Review" 2014, vol. 30(2), s. 190–195.

[8] J. Apanowicz, *Metodologia ogólna*, Wyższa Szkoła Administracji i Biznesu, Gdynia 2002.

[9] B. Desmond, J. Richards, R. Allen, A.G. Lowe-Norris, *Active Directory: Designing, Deploying, and Running Active Directory*, O'Reilly Media, Sebastopol 2008.

próbę ich odszyfrowania za pomocą programu LOphtCrack v6.0.15. Podobne testy były wykonywane przez J.A. Caziera i B.D. Medlin[10]. Dotyczyły one jednak systemów *e-commerce*. Zastosowano też zupełnie różną kategoryzację i skalę ocen siły hasła.

Wdrożenie zostało poprzedzone akcją ankietową, podczas której zebrano informacje o sposobie tworzenia, zmiany i zapamiętywania haseł przez użytkowników. Respondentami byli urzędnicy, których hasła systemowe były poddawane testom. Ankietowani anonimowo wyrażali także opinię o alternatywnych sposobach logowania, takich jak techniki biometryczne, behawioralne, tokeny czy karty kryptograficzne. Oceniali też zasadność wprowadzenia kontroli złożoności haseł. Dodatkowo ankiety zostały wysłane do wszystkich jednostek samorządowych położonych na terytorium Polski. Nie były one anonimowe. Zawarte w nich pytania dotyczyły głównie stosowanych usług katalogowych, algorytmów szyfrujących oraz użytkowanych obecnie i planowanych w przyszłości metod autoryzacji.

Na podstawie zebranego, obszernego materiału badawczego została wybrana alternatywna metoda uwierzytelniania. Rozesłana ankieta zweryfikowała jej przydatność oraz funkcjonalność. Z respondentami, którzy negatywnie ocenili zaproponowaną metodę, przeprowadzono wywiad w celu sprecyzowania ich oczekiwań. Po jej modyfikacji opracowano prototyp modułu logowania. Proste oprogramowanie symulujące proces logowania oraz ustalania i zmiany jego parametrów zostało przedstawione respondentom do zaopiniowania.

3. Przebieg badań

Badania rozpoczęto w styczniu 2013 r. od rozprowadzenia wśród wszystkich pracowników wybranej instytucji anonimowych ankiet. Zawierały one sześć pytań, spośród których dwa były półotwarte, pozostałe zaś to pytania zamknięte. Zwrócono 181 ankiet, co stanowi 56,56%. Część z nich (pięć) zawierała błędy polegające na braku odpowiedzi na niektóre pytania. Tak niski zwrot może być tłumaczony tym, iż ankietowani nie przywiązywali wagi do badań lub pomimo zapewnienia o anonimowości obawiali się udzielić informacji[11].

[10] J.A. Cazier, B.D. Medlin, *How secure is your password? An analysis of e-commerce passwords and their crack times*, „Journal of Information System Security" 2006, vol. 2(3), s. 69–82.

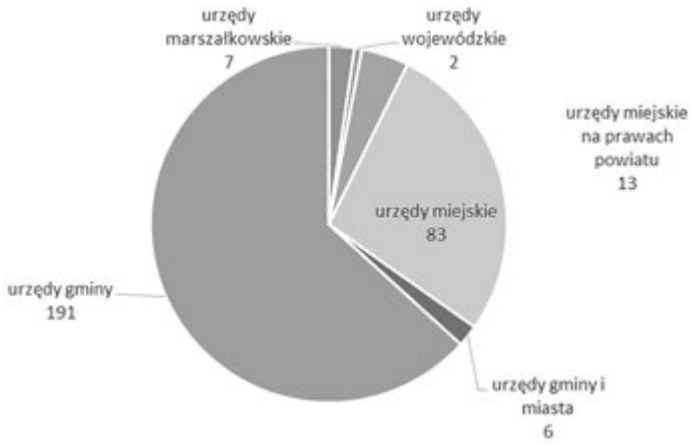
[11] R.M. Groves, J. Fowler, M.P. Couper, J.M. Lepkowski, E. Singer, R. Tourangeau, *Survey Methodology*, John Wiley&Sons Inc., Hoboken 2009.

W tym samym czasie rozpoczęto testowanie siły haseł przez próbę ich odszyfrowania. Należy zaznaczyć, iż w badanej organizacji ustanowiono *Politykę bezpieczeństwa*. Jej zapisy jasno precyzowały, że użytkownicy winni stosować hasła o długości nie mniejszej niż osiem znaków, zawierające trzy z czterech dostępnych grup znaków. Grupy te to małe i duże litery, cyfry oraz znaki specjalne.

Jednocześnie zakazane było stosowanie w haśle imion, nazwisk, dat związanych z użytkownikiem lub członkami jego rodziny, jak również wyrazów słownikowych. Urzędnicy zobligowani byli do comiesięcznej zmiany hasła. Funkcjonujący w organizacji system informatyczny oparty na usługach katalogowych Windows serwer 2003 nie kontrolował złożoności oraz historii haseł.

Do wszystkich użytkowników, których hasła zostały złamane, wysłano drogą mailową informację z wiadomością, że ich hasła nie spełniają wymogów określonych w *Polityce bezpieczeństwa*. Po miesiącu ponowiono testy, a także wysłanie informacji mailowych, które uzupełniono o przytoczone z *Polityki bezpieczeństwa* zasady konstruowania i posługiwania się hasłami. Również w kolejnym miesiącu wykonano testy, a następnie włączono w *Active Directory* kontrolę złożoności i historii haseł. Próby łamania haseł były wykonywane jeszcze trzykrotnie, w miesięcznych odstępach.

Pod koniec 2013 r. rozesłano mailowo do wszystkich jednostek samorządowych na szczeblu gminy oraz urzędów wojewódzkich i marszałkowskich ankiety z 12 pytaniami zamkniętymi. Na 2424 wysłane ankiety zwrócono 302, czyli 12,46%. Na rysunku 1 pokazano ich liczbę w podziale na poszczególne rodzaje instytucji.



Rysunek 1. Liczba zwróconych ankiet w podziale na poszczególne rodzaje instytucji

Źródło: opracowanie własne.

Maile były podpisane certyfikatem cyfrowym. Zawierały także w treści numer telefonu, pod którym można było uzyskać dodatkowe informacje związane z ankietami. Elementy te miały na celu uwiarygodnienie prowadzonych badań. W pięciu przypadkach okazały się one niewystarczające. Zażądano dokumentów świadczących o związku osoby prowadzącej badania z Uniwersytetem Gdańskim.

Stosunkowo małą liczbę zwróconych ankiet można tłumaczyć niechęcią do podawania szczegółów autoryzacji, które mogą zagrozić bezpieczeństwu systemu informatycznego. Wybór formy e-mail miał także niekorzystny wpływ. Poczta elektroniczna nie jest uznawana za oficjalną drogę składania pism urzędowych. Zauważono, że niektóre skrzynki mailowe instytucji odrzucają wiadomości z powodu przepełnienia, co świadczy o tym, że urzędnicy sprawdzają je zbyt rzadko. Z tego też powodu w czterech przypadkach w celu doręczenia ankiet posłużono się ePUAP (elektroniczną platformą usług administracji publicznej), oficjalnym systemem udostępnionym przez Ministerstwo Administracji i Cyfryzacji służącym komunikacji z organizacjami publicznymi. Nie został on użyty w badaniach na większą skalę ze względu na brak listy adresowej elektronicznych skrzynek podawczych systemu oraz trudności w automatyzacji wysyłki.

Spośród 302 odpowiedzi 29 (9,6%) zawierało jedynie dane ogólne, niedotyczące bezpośrednio zagadnień związanych z bezpieczeństwem. Dołączono do nich wiadomość, iż funkcjonująca w organizacji *Polityka bezpieczeństwa* zabrania przekazywania informacji, które mogą być pomocne w uzyskaniu nieautoryzowanego dostępu do systemu informatycznego. Tak sformułowana odpowiedź była istotna dla prowadzonych badań, gdyż świadczyła, że w instytucji ustanowiono *Politykę bezpieczeństwa*, a jej postanowienia są przestrzegane.

W lutym 2014 r. zaproszono 10 urzędników przypadkowo spotkanych na korytarzu jednej z instytucji do poddania się testom na zapamiętywanie losowych ciągów alfanumerycznych. Testy zostały oparte na specjalnie utworzonym w tym celu oprogramowaniu. Wylosowano po 10 ciągów 4-, 5-, 6-, 7- i 8-znakowych. Każdy ciąg musiał zawierać przynajmniej jeden niepowtarzalny znak z każdej z grup. Wylosowane ciągi były wspólne dla każdej próby. Badanym wyświetlano kolejno pojedynczo ciągi, począwszy od najkrótszych. Pozostawiono ich decyzji to, jakiego czasu potrzebują, by uzyskać przekonanie, że poprawnie je zapamiętali. Zadaniem badanego było odtworzenie ciągu bezpośrednio po jego zniknięciu. Mógł on także przerwać test, gdy uznał, że nie jest już w stanie zapamiętać ciągów określonej długości. Ponieważ testy były prowadzone na stanowiskach oraz w godzinach pracy, uwzględniały wszelkie rozpraszające uwagę czynniki.

W marcu 2014 r. w jednej z instytucji wszystkim użytkownikom systemu informatycznego rozesłano propozycję nowego sposobu konstruowania haseł. Wygenerowano tabelę, 10x10, zawierającą 100 znaków alfanumerycznych, po jednym w każdej

komórce. Zaproponowano, aby ją wydrukować i na jej podstawie, kreśląc w myślach kształty, tworzyć hasła. Propozycja zawierała również prośbę o opinię, która została skategoryzowana w następujący sposób:

- metoda nieprzydatna;
- metoda przydatna, ale będę stosować własną, gdyż jest ona prostsza;
- metoda przydatna i będę ją stosował/a.

Jedynie 79 osób z 320, czyli 24,69%, ustosunkowało się do propozycji. Ze wszystkimi, którzy uznali metodę za nieprzydatną, przeprowadzono wywiad mający na celu zebranie uwag.

Opracowano prototyp logowania w postaci aplikacji, którą przedstawiono 10 respondentom negatywnie oceniającym nowy sposób autoryzacji oraz 10 preferującym hasła pomimo przydatności proponowanej metody. Aplikacja dla każdego użytkownika generowała unikalną tabelę 10x10 ze znakami alfanumerycznymi. Pozwalała na oznaczanie za pomocą myszy lub klawiatury poszczególnych jej pól. Oznaczone pola czytane od lewej do prawej tworzyły hasło przekazywane do systemu. Na potrzeby logowania przechowywane były zarówno hasło, jak i tabela. Zebrano opinie użytkowników i przeanalizowano utworzone przez nich hasła.

4. Wyniki badań

Przeprowadzona wśród użytkowników ankieta pozwala na stwierdzenie, iż jedynie 12% z nich stosuje się do postanowień funkcjonującej w ich organizacji *Polityki bezpieczeństwa*, mówiących o zasadach konstruowania bezpiecznych haseł. Zasady te, zgodne z dobrymi praktykami, zakazują tworzenia haseł zawierających daty, imiona czy wyrazy w języku polskim lub angielskim, jak również znaki ułożone w przewidywalnej kolejności. Mają one na celu zapobieżenie szybkiemu złamaniu ich przez ataki słownikowe, statystyczne[12] oraz odgadnięciu ich przez działania socjotechniczne[13]. Ankietowani (16 osób) stosowali bezpieczne hasła, budując je na podstawie znaków przypadkowo przychodzących im na myśl. Jeden respondent wspomagał się generatorem haseł, a pięciu budowało hasło przy wykorzystaniu sentencji, czyli pierwszych liter każdego z wyrazu składającego się na sentencję. Pozostali wykorzystywali ważne

[12] S. Schechter, C. Herley, M. Mitzenmacher, *Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks*, w: *Proceedings of the 5th USENIX conference on hot topics in security*, red. I. Goldberg, USENIX Association, Washington 2010, s. 1–8.

[13] C. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2012.

dla nich informacje lub stosowali ciągi kolejnych znaków. Szczegółowe zestawienie technik stosowanych w celu utworzenia hasła przedstawia tabela 1.

Tabela 1. Zestawienie technik tworzenia haseł

Deklarowana metoda konstruowania haseł	Liczba	Udział procentowy
Generator haseł	1	0,55
Przypadkowe znaki	16	8,84
Fragmenty sentencji	5	2,76
Ciągi kolejnych znaków	37	20,44
Częścią hasła są informacje personalne	44	24,31
Częścią hasła są wyrazy	39	21,55
Stosowanych jest kilka z powyższych metod jednocześnie	39	21,55

Źródło: opracowanie własne.

Postanowiono sprawdzić, jaki wpływ ma deklarowany, niezgodny z zasadami bezpieczeństwa sposób tworzenia haseł na możliwość ich złamania. W okresie połowy roku co miesiąc były podejmowane próby złamania haseł 254 kont. Pominięto konta m.in. wyższego kierownictwa oraz osób zajmujących się przetwarzaniem danych niejawnych. Wyniki przedstawiono w tabeli 2.

Tabela 2. Wyniki testów łamania haseł

Numer testu	Liczba złamanych	Liczba częściowo złamanych	Liczba haseł o długości poniżej ośmiu znaków
Test 1	230	14	112
Test 2	222	20	104
Test 3	190	45	77
Test 4	164	80	0
Test 5	164	76	0
Test 6	162	79	0

Źródło: opracowanie własne.

Pierwsza próba była dokonywana bez uprzedzenia użytkowników. Ponad 90% haseł zostało złamanych, a w pięciu odgadnięto co najmniej jeden znak. Kolejne testy wykonano po powiadomieniu użytkowników o słabości ich haseł, a następnie przywołaniu odpowiednich zapisów z *Polityki bezpieczeństwa*, co jedynie nieznacznie poprawiło sytuację. Znaczny spadek liczby złamanych haseł zaobserwowano dopiero w teście 4, który został poprzedzony włączeniem kontroli złożoności w *Active Directory*. Nawet wówczas prawie 65% haseł nie można uznać za bezpieczne. Jedną z przyczyn

jest zastosowanie przestarzałego protokołu uwierzytelniania LM lub NTLM zamiast znacznie bezpieczniejszego NTLMV2[14].

Same zasady złożoności nie stanowią jednak wystarczającego zabezpieczenia przed atakami hybrydowymi, czyli wykorzystującymi hasła pobrane ze słownika, a uzupełnione, poprzedzone lub przeplatane ciągami cyfrowymi. Postanowiono więc zweryfikować metody tworzenia haseł deklarowane przez użytkowników oraz sprawdzić, w jaki sposób je zmieniają. Do kontroli wybrano 132 konta użytkowników, których hasła udało się złamać podczas wszystkich 6 testów oraz które ulegały regularnym zmianom.

Najczęściej użytkownicy zawierają w hasłach imiona i nazwiska swoje lub bliskich sobie osób. Jedynie w 17% nie udało się ustalić sposobu budowania haseł. Szczegółowe dane zostały przedstawione w tabeli 3.

Tabela 3. Zweryfikowany sposób tworzenia haseł

Zidentyfikowana metoda tworzenia haseł	Udział procentowy
Częścią hasła są informacje personalne	49
Częścią hasła są wyrazy	26
Ciągi kolejnych znaków	8
Inne	17

Źródło: opracowanie własne.

Uzyskane rezultaty jasno wskazują, że nawet znajomość *Polityki bezpieczeństwa* w połączeniu z przedstawionymi dowodami słabości haseł nie jest w stanie skłonić użytkowników do konstruowania bardziej bezpiecznych haseł. Urzędnicy nie identyfikują się z problemem potencjalnego dostępu do danych przez nieuprawnioną autoryzację z wykorzystaniem ich kont w systemie informatycznym[15].

W związku z zaprezentowanymi powyżej rezultatami postanowiono sprawdzić, jak przedstawia się autoryzacja dostępu do systemów informatycznych pozostałych jednostek samorządowych. Większość (76%) wykorzystuje hasła jako jedyny element autoryzacji. Pozostałe korzystają również z tokenów, kart kryptograficznych, a jeden nawet z technik behawioralnych[16].

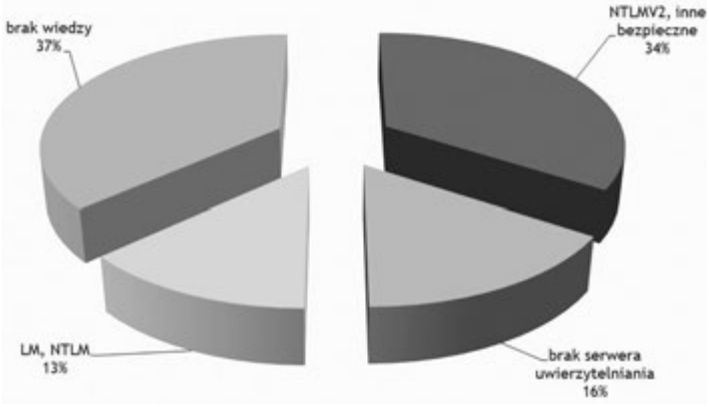
---

[14] J. De Ciercq, *Deflecting Active Directory Attacks*, w: *ISSE 2006 – Securing Electronic Business Processes*, red. S. Sachar Paulus, N. Pohlmann, H. Reimer, Springer, Heidelberg 2006, s. 168–175.

[15] B. Bulgurcu, H. Cavusoglu, I. Benbasat, *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*, „MIS Quarterly" 2010, vol. 34(3).

[16] H. Gamboa, A. Fred, *A behavioral biometric system based on human-computer interaction*, w: *Biometric Technology for Human Identification,* red. A.K. Jain, N.K. Ratha, SPIE, vol. 5404, 2004, s. 381–392.

Zaobserwowano jednak, iż powszechność wykorzystywania haseł nie pociąga za sobą dbałości o ich bezpieczeństwo. Zaskoczeniem był dla badacza fakt, iż niektóre z jednostek nie mają serwera, dzięki któremu można byłoby kontrolować zasady złożoności. Wśród pozostałych duża liczba stosuje protokoły autentykacji LM lub NTLM. Są one przestarzałe i podatne na kryptoanalizę[17]. Szczegółowe dane dotyczące stosowanych przy autoryzacji protokołów w badanych jednostkach samorządowych przedstawiono na rysunku 2.



Rysunek 2. Uwierzytelnianie stosowane w badanych jednostkach

Źródło: opracowanie własne.

Interesującym faktem w tych jednostkach jest brak wiedzy odnoszącej się do stosowanych algorytmów. Wynika on przypuszczalnie z niskich kompetencji służb informatycznych, nadmiernego ich obciążenia obowiązkami lub niedbałością. Tezę o niedbałości potwierdzają wyniki testów penetracyjnych sieci teleinformatycznych urzędów. Wyniki tych testów wskazywały, że najbardziej podatne na zagrożenia są komputery użytkowane przez informatyków ze względu na brak aktualizacji wielu krytycznych aplikacji[18].

Jeśli więc stosowanie haseł wiąże się z dużymi problemami, należy się zastanowić nad możliwością zastosowania alternatywnych form uwierzytelniania. Pomimo że we wszystkich badanych jednostkach podstawową techniką uwierzytelniania są hasła, to stosowane były też karty kryptograficzne oraz tokeny. Techniki biometryczne

[17] M. Bakker, R. Van Der Jagt, *GPU-based password cracking*, University of Amsterdam, System and Network Engineering, Amsterdam 2010.

[18] P. Jatkiewicz, *Identifying Factors of an Information Security Management System of Local Self-government Bodies*, w: *Information Systems: Development, Learning, Security*, red. S. Wrycza, Springer, Berlin–Heidelberg 2013, s. 50–65.

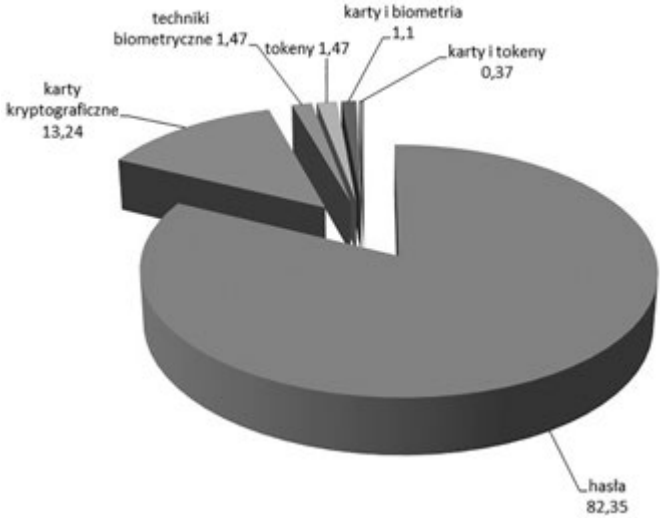
wykorzystywane są marginalnie. Szczegółowe dane dotyczące stosowanych technik uwierzytelniania przedstawia tabela 4.

Tabela 4. Stosowane techniki uwierzytelniania

Techniki	Aktualnie stosowane
Hasła	272
Karty kryptograficzne	45
Techniki biometryczne	4
Tokeny	17
Techniki behawioralne	1

Źródło: opracowanie własne.

Jedynie 17,65% badanych urzędów zdecydowałoby się na całkowite wyeliminowanie haseł i zastąpienie ich innymi technikami. Większość z nich zastosowałaby karty kryptograficzne. Szczegóły zawiera rysunek 3.



Rysunek 3. Deklarowane techniki uwierzytelniania zastępujące hasła w badanych organizacjach

Źródło: opracowanie własne.

5. Podsumowanie

Przedstawione badania dają podstawę do stwierdzenia, że hasła są dominującą formą uwierzytelniania w systemach informatycznych eksploatowanych przez instytucje samorządowe. Biorąc pod uwagę szczupłość zasobów finansowych, jakie są w stanie przeznaczyć urzędy na wdrożenie i utrzymanie rozwiązań informatycznych, problemy z kadrą informatyczną, jak również niechęć użytkowników, należy stwierdzić, że wprowadzenie popularnych, dostępnych na rynku technik uwierzytelniania wydaje się mało realne w najbliższej przyszłości. Wobec tego należy się skupić nad głównymi zdiagnozowanymi problemami związanymi ze stosowaniem haseł, tzn. słabością użytkowanych algorytmów oraz zdolnością do tworzenia i zapamiętywania przez użytkowników haseł spełniających wymogi bezpieczeństwa.

Dla przypomnienia – słabe algorytmy były eksploatowane ze względu na brak wiedzy o możliwości zaimplementowania silniejszych. Nasuwa się więc wniosek o konieczności weryfikowania kompetencji informatyków samorządowych. Samo wykształcenie nie jest już dostatecznym kryterium oceny, gdyż poziom nauczania na uczelniach jest bardzo zróżnicowany. Producenci komponentów systemu informatycznego, co do zasady, winni stosować najsilniejsze algorytmy kryptograficzne jako domyślne parametry startowe. W przypadku ich aktualizacji zachodzi konieczność skutecznego poinformowania użytkowników o możliwości zastosowania nowych opcji.

Proces zapamiętywania złożonych ciągów alfanumerycznych, jakimi są bezpieczne hasła, można wspomóc. Dlatego też postanowiono zaproponować użytkownikom budowę haseł na podstawie wspominanej już tablicy znaków. Jedynie 14% procent respondentów określiło tę metodę jako nieprzydatną. Równocześnie tylko 13% zadeklarowało, że będzie jej używać. Pozostali dostrzegali jej zalety, lecz woleli dotychczasową stosowaną przez siebie metodę.

Podczas wywiadu z 10 przypadkowymi respondentami zwrócono uwagę na kłopot, jakim jest odczyt znaku z wydrukowanej tabeli oraz odnalezienie go na klawiaturze. Czynność ta znacznie wydłuża proces logowania i prowadzi do licznych pomyłek. Dodatkowo wydrukowana kartka może się zagubić wśród licznych przetwarzanych dokumentów. Znaczącym ułatwieniem byłoby wyświetlanie tabeli na ekranie oraz dokonywanie wyboru znaków za pomocą myszy lub palcem na ekranie dotykowym.

Zgodnie z sugestią respondentów, opracowano prototyp systemu autoryzacji w postaci aplikacji, która symulowała proces logowania. Poproszono 10 z nich, którzy uważali przedstawioną metodę za nieprzydatną, oraz 10 uznających jej przydatność, ale preferujących własną metodę o przetestowanie rozwiązania i wyrażenie opinii. Wszyscy testerzy mieli wygenerować po 10 haseł i za ich pomocą zalogować się.

Żadne z utworzonych przez nich haseł nie było krótszych niż 10 znaków, a średnia długość wynosiła 13. Z oczywistych względów wszystkie spełniały najbardziej rygorystyczne zasady. Nie były oparte na imionach, nazwiskach czy wyrazach. Nie nawiązywały też w żaden sposób do poprzednich. Ponieważ dla każdego użytkownika i każdej zmiany hasła losowana była zawartość tabeli znaków, wśród 200 wygenerowanych haseł żadne nie powielało się.

Choć przedstawiona metoda nie jest bez wad (oprócz szyfrowania hasła należy także przechowywać bezpiecznie tabele znaków, łatwiej też jest podejrzeć rysowany na tabeli kształt), to jednoznacznie można stwierdzić, że opinia, iż hasła są „martwe", jest przedwczesna. Ich potencjał nadal można wykorzystywać, a metody ich tworzenia i użytkowania udoskonalać.

Bibliografia

Apanowicz J., *Metodologia ogólna*, Wyższa Szkoła Administracji i Biznesu, Gdynia 2002.

Bakker M., Van Der Jagt R., *GPU-based password cracking*, University of Amsterdam, System and Network Engineering, Amsterdam 2010.

Bulgurcu B., Cavusoglu H., Benbasat I., *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*, „MIS Quarterly" 2010, vol. 34(3).

Calder A., *Implementing Information Security Based on ISO 27001/ISO 17799: A Management Guide*, Van Haren Publishing, Zalthommel 2006.

Cazier J.A., Medlin B.D., *How secure is your password? An analysis of e-commerce passwords and their crack times*, „Journal of Information System Security" 2006, vol. 2(3), s. 69–82.

De Clercq J., *Deflecting Active Directory Attacks*, w: *ISSE 2006 – Securing Electronic Business Processes*, red. S. Sachar Paulus, N. Pohlmann, H. Reimer, Springer, Heidelberg 2006, s. 168–175.

Desmond B., Richards J., Allen R., Lowe-Norris A.G., *Active Directory: Designing, Deploying, and Running Active Directory*, O'Reilly Media, Sebastopol 2008.

Dmitrienko A., Liebchen C., Rossow C., Sadeghi A.R., *On the (in) security of mobile two-factor authentication*, Technical Report TUD-CS-2014-0029, 2014.

Gamboa H., Fred A., *A behavioral biometric system based on human-computer interaction*, w: *Biometric Technology for Human Identification*, red. A.K. Jain, N.K. Ratha, SPIE, vol. 5404, 2004, s. 381–392.

Gosney J., *Password Cracking HPC*, Passwords^12 Conference, Oslo 2012.

Groves R.M., Fowler J., Couper M.P., Lepkowski J.M., Singer E., Tourangeau R., *Survey Methodology*, John Wiley&Sons Inc., Hoboken 2009.

Hadnagy C., *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2012.

Herley C., Van Oorschot P., *A research agenda acknowledging the persistence of passwords*, „Security & Privacy IEEE" 2012, vol. 10(1), s. 28–36.

Jatkiewicz P., *Identifying Factors of an Information Security Management System of Local Self-government Bodies*, w: *Information Systems: Development, Learning, Security*, red. S. Wrycza, Springer, Berlin–Heidelberg 2013, s. 50–65.

Mikkonen T., *Perceptions of controllers on EU data protection reform: A Finnish perspective*, „Computer Law & Security Review" 2014, vol. 30(2), s. 190–195.

Schechter S., Herley C., Mitzenmacher M., *Popularity is everything: A new approach to protecting passwords from statistical-guessing attacks*, w: *Proceedings of the 5th USENIX conference on hot topics in security*, red. I. Goldberg, USENIX Association, Washington 2010, s. 1–8.

Sobczak J., *Prawne uregulowania obowiązujące przedsiębiorstwa w zakresie bezpieczeństwa informacji oraz skutki ich naruszenia*, „Zeszyty Naukowe Uczelni Vistula" 2014, nr 35, s. 99–114.

Vance A., *If your password is 123456, just make it hack me*, „The New York Times" 2010, no. 20.

* * *

Authentication methods in the information systems of local governments

Summary

The paper presents the results of studies conducted in local government entities in Poland. The study focused on the authentication of users in information systems; the survey was addressed to users and organizations. The interviews conducted with the civil servants were followed by an attempt to crack their user account passwords by means of brute force, dictionary attacks and hybrid attacks. The study helped to identify the key factors influencing the construction of weak passwords. An alternative method of authentication was presented. The effectiveness of the new method was verified. A prototype of the authorization system in the form of a program was made available to users for evaluation.

Keywords: authorization, passwords, information security