Nowa Biblioteka. Usługi, Technologie Informacyjne i Media 2018, nr 4 (31), s. 37–50
ISSN 2451-2575 (wersja elektroniczna)
http://www.nowabiblioteka.us.edu.pl/
GICID 71.0000.1500.0677

Wojciech Balawender
student I roku informatyki magisterskiej
Wydział Informatyki i Nauki o Materiałach
Koło Naukowe Infologów
Instytut Bibliotekoznawstwa i Informacji Naukowej
Uniwersytet Śląski w Katowicach
e-mail: wbalawen@us.edu.pl

Siła haseł w kontekście ochrony zbiorów danych

Abstrakt: W artykule podjęto temat porównywania jakości haseł za pomocą entropii informacyjnej. Wyszczególniono kluczowe regulacje prawne obowiązujące administratorów baz danych. Zaprezentowano niektóre metody przechwytywania i łamania haseł oraz omówiono elementarne zasady bezpieczeństwa, do których powinien stosować się każdy użytkownik komputera, w tym mnemotechniczne metody tworzenia silnych haseł. Przeprowadzono analizę zabezpieczeń procesów identyfikacyjnych siedmiu największych banków.

Słowa kluczowe: Baza danych. PUODO. RODO. Siła hasła

Stan prawny

W Polsce każdy podmiot przetwarzający dane osobowe w zbiorze jako administrator (z wyłączeniem sytuacji ujętych w art. 43 ust. 1 pkt 1–11 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*) był zobowiązany do rejestracji tego zbioru u Generalnego Inspektora Ochrony Danych Osobowych (GIODO) (*Rozporządzenie*, 2004, poz. 1024). Z dniem 25 maja 2018 r., na skutek ustawy przyjętej w wyniku *Rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 2016/679 z dnia 27 kwietnia 2016 r.* (RODO) urząd ten został zastąpiony przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO), a obowiązek zgłaszania zbiorów danych został zniesiony. RODO nakłada obowiązek prowadzenia rejestru czynności przetwarzania danych, nie

precyzuje jednak, w jaki sposób należy je zabezpieczać, ani jakie kryteria muszą spełniać hasła systemów informatycznych, aby zostały uznane za bezpieczne. Szczegółowe wytyczne zostały zawarte w *Rozporządzeniu 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*. W świetle tych przepisów hasło chroniące dane powinno składać się co najmniej z sześciu dowolnych znaków dla podstawowego poziomu bezpieczeństwa (*Rozporządzenie*, 2004, zał. A, IV pkt 2) oraz co najmniej z ośmiu znaków (wśród nich małe i wielkie litery oraz cyfry lub znaki specjalne) dla podwyższonego poziomu bezpieczeństwa (*Rozporządzenie*, 2004, zał. B, VIII). Dodatkowy środek bezpieczeństwa stanowi obowiązek zmiany hasła co 30 dni (*Rozporządzenie*, 2004, zał. A, IV pkt 2).

System informatyczny musi zostać tak skonstruowany, by dopuszczalne było wykorzystywanie haseł zgodnych z *Rozporządzeniem*, nie ma natomiast obowiązku ich wymuszania poprzez rozwiązania technologiczne. Wspomniane regulacje mogą być przekazywane pracownikom obsługującym dane osobowe w dowolny sposób, np. podczas szkolenia. Niemniej podczas rejestracji nowych kont w serwisach internetowych powszechnie stosuje się systemy walidacji haseł, które mają na celu zwiększenie bezpieczeństwa konta. Skrypty odrzucają tzw. słabe hasła, czyli zbyt krótkie, składające się z ciągu tych samych znaków lub będące powtórzeniem identyfikatora. Zmniejsza to prawdopodobieństwo przejęcia kontroli nad kontem przez osobę nieuprawnioną. Celem artykułu, w związku z tak zarysowanym problemem, jest zaprezentowanie metody szacowania siły haseł za pomocą entropii informacyjnej, czyli wielkości określającej średnią ilość informacji przypadającej na pojedynczą wiadomość – hasło, oraz zwrócenie uwagi na zagrożenia związane z wykorzystywaniem haseł w internecie (*Entropia*).

Badanie siły hasła

Siłę haseł można wyrazić w postaci wzoru na poziom entropii informacyjnej[1]:

[1] W artykule wykorzystano wzór na entropię z logarytmem o podstawie 2 (badana jest entropia w bitach).

$$H(X) = -\sum_{i=1}^{k} p(x_i) log_2\, p(x_i)$$

Źródło: Opracowanie własne na podstawie: (Borda, 2011).

X oznacza zmienną losową o zbiorze wartości $\{x_1, x_2, \ldots, x_k\}$, a $p(x_i)$ to prawdopodobieństwo zajścia zdarzenia x_i. Zakładając, że prawdopodobieństwo wystąpienia każdego znaku jest takie samo (hasła generowane są w sposób losowy), do obliczenia entropii możemy wykorzystać uproszczony wzór:

$$H(X) = log_2(n)$$

Źródło: Opracowanie własne na podstawie: (Borda, 2011).

w którym n oznacza moc zbioru użytego do wygenerowania hasła.

Tabela 1. Przykładowe wartości entropii dla haseł zbudowanych z różnych zbiorów znaków

Zbiór	Hasło sześcioznakowe		Hasło ośmioznakowe		Hasło dwunastoznakowe	
	kombinacje	entropia	kombinacje	entropia	kombinacje	entropia
Cyfry (0–9)	10^6	19.93	10^8	26.57	10^{12}	39.86
Alfabet łaciński	26^6	28.20	26^8	37.60	26^{12}	56.40
Alfabet łaciński CS*	52^6	34.20	52^8	45.60	52^{12}	68.40
Alfabet łaciński CS + cyfry	62^6	35.72	62^8	47.63	62^{12}	71.45
ASCII (drukowalne)	95^6	39.41	95^8	52.55	95^{12}	78.83
ISO 8859-2 CS	191^6	45.46	191^8	60.61	191^{12}	90.92
Unicode**	136755^6	102.36	136755^8	136.48	136755^{12}	204.73

* CS – ang. *case sensitivity*; wielkie i małe litery są traktowane jako różne znaki.
** Liczba znaków w wersji standardu 10.0 wynosi 136 755 (czerwiec 2017 r.).

Źródło: Opracowanie własne.

Obliczenie wartości entropii pozwala porównywać siły haseł. Większa wartość oznacza, że hasło trudniej będzie odgadnąć. Należy zauważyć, iż sama wiedza o liczbie kombinacji, jakie można utworzyć z określonego zbioru, może być niewystarczająca do porównywania haseł w przypadku, gdy prawdopodobieństwa wystąpienia znaków w porównywanych hasłach są różne. A zatem posługiwanie się wartością entropii jest bardziej praktyczne i miarodajne. Najniższa teoretyczna entropia hasła spełniającego wytyczne zawarte w *Rozporządzeniu* w systemie o podwyższonym stopniu bezpieczeństwa (8 znaków liter alfabetu łacińskiego CS + cyfry) wynosi 47,63 (zob. tabela 1). W rzeczywistości, z uwagi na powszechne preferencje, hasła tworzone przez ludzi cechują się znacznie niższą entropią (umieszczanie wielkiej litery na początku, liczby określającej rok urodzenia na końcu etc). Ten fakt wykorzystywany jest przez crackerów (osoby zajmujące się łamaniem zabezpieczeń komputerowych) podczas siłowego łamania haseł. Korzystają oni z tzw. masek, które ograniczają przeszukiwany zbiór znaków na poszczególnych pozycjach, co znacząco redukuje liczbę testowanych kombinacji (*Mask*).

Załóżmy jednak najbardziej pesymistyczny wariant, w którym sprawdzone muszą zostać wszystkie ciągi ($62^8 \approx 218$ bilionów kombinacji). Czy to wystarczająco dużo? W dniu ogłoszenia *Rozporządzenia* – prawdopodobnie tak. Ówczesna najszybsza dostępna w sprzedaży karta graficzna, której procesor mógłby pomóc w łamaniu hasła, oferowała moc obliczeniową na poziomie „zaledwie" 17,3 GFLOPS (*ATI*, 2018). Jednak współczesna karta gamingowa GTX 1080 Ti oferuje już 11,3 TFLOPS (ponad 650-krotny wzrost wydajności) (*NVIDIA*, 2017). Korzystając z tego układu, bezpłatne, proste w obsłudze programy do łamania haseł (np. Hascat na licencji MIT, obsługujący większość popularnych kryptograficznych funkcji skrótu, które z ciągu danych o dowolnej długości generują n-bitowy skrót, tzw. *hash*) bez problemu mogą obliczyć wiele miliardów haszów w ciągu jednej sekundy[2]. Oznacza to, że siłowe sprawdzenie wszystkich ośmioznakowych kombinacji może zająć kilka godzin[3]. Warto wspomnieć, że w zasięgu średniozaawansowanego crackera dostępne są także tzw. tęczowe tablice (ang. *rainbow tables*), które

[2] Przeciętny czas potrzebny do obliczenia przez układ popularnej funkcji skrótu SHA-1 na podstawie przeprowadzonego przez Jeremiego Gosneya Benchmarku, w którym użyto klastra złożonego z ośmiu kart graficznych (wybrano najgorszy wynik, tj. 8511 MH/s – około 8,5 miliarda haszów na sekundę) (*8x Nvidia*, 2018).

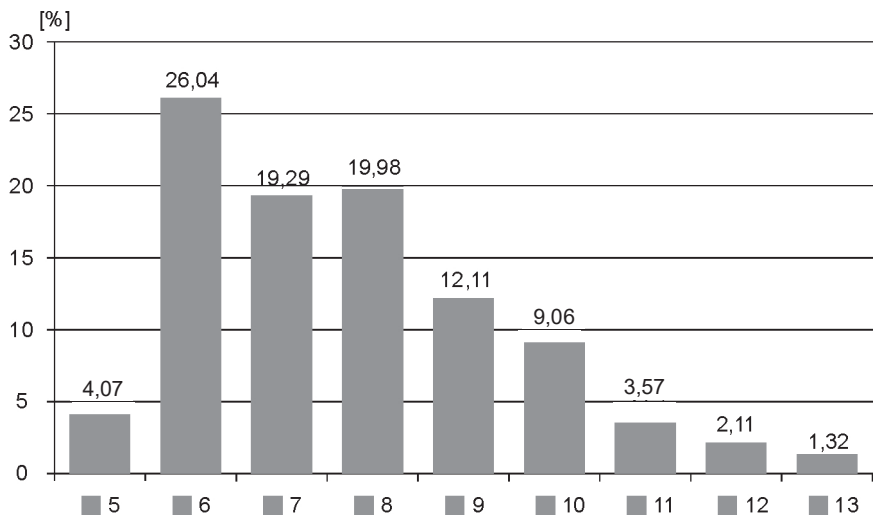
[3] Metodologia obliczeń: liczba wszystkich ośmiowyrazowych wariacji z powtórzeniami zbioru 62-elementowego / szybkość obliczania haszów SHA1 = $62^8 / 8{,}5 \times 10^9 \approx 7$ godzin.

z blisko stuprocentowym prawdopodobieństwem pozwalają skrócić proces crackowania do kilku minut[4]. Jest to możliwe, ponieważ tęczowe tablice zawierają już obliczone skróty, w związku z czym oszczędzana jest moc procesora niezbędna do obliczeń.

W świetle tych faktów nie można uznać wymagań ministerialnych narzuconych administratorom za restrykcyjne. Zwiększająca się moc komputerów osobistych powinna skłonić polski sejm do zmiany minimów zawartych w *Rozporządzeniu* celem poprawy bezpieczeństwa kont administratorów.

Tworzenie bezpiecznego hasła

Firma Imperva, zajmująca się bezpieczeństwem cybernetycznym i ochroną danych korporacyjnych, przeanalizowała 32 miliony haseł, które wykradziono z bazy RockYou.com (*Consumer*, 2014).



Wykres 1. Procentowy rozkład długości haseł

Źródło: Opracowanie własne na podstawie: (*Consumer*, 2014, s. 2).

Z analizy tych danych (wykres 1) wynika, że ponad 69% użytkowników serwisu wykorzystuje hasła o długości od 5 do 8 znaków. Jak już wspomniano, takie hasła nie zapewniają należytego poziomu ochrony.

[4] Wydajność poszczególnych tablic można obejrzeć, wybierając element z kolumny „performance" (*RainbowCrack*, 2017).

Oczywiście niektóre systemy informatyczne są wyposażone w dodatkowe środki bezpieczeństwa, takie jak blokowanie konta po kilku próbach autoryzacji zakończonych niepowodzeniem lub – w przypadku serwisów internetowych – generowanie dodatkowego zadania (CAPTCHA, odpowiedź na pytanie kontrolne etc.), co znacząco utrudnia ataki zdalne. Tutaj mamy jednak do czynienia z wyciekiem całej bazy danych. Nawet jeśli hasła w bazie były (a zawsze powinny być) przechowywane w formie zahaszowanej, jedynym ograniczeniem dla przestępcy działającego na lokalnej bazie danych jest moc obliczeniowa wykorzystanego sprzętu. Słabe hasło szybko zostanie złamane, co może prowadzić do przejęcia kontroli nad kontem. Sytuacja staje się jeszcze bardziej niepokojąca, gdy używamy tego samego hasła w kilku miejscach.

Istnieją dwie dobre metody tworzenia bezpiecznych haseł. Pierwszą jest skorzystanie z generatora (np. generator Online pod adresem https://passwordsgenerator.net). Metoda ta sprawdza się w sytuacji, gdy nie musimy takiego hasła pamiętać (np. w przypadku hasła zapisanego w pliku konfiguracyjnym aplikacji języka PHP, komunikującej się z bazą MySQL). Jednak posługiwanie się na co dzień bezpiecznym hasłem typu „$N6!”P6~sB9`nT2]” podczas logowania do konta pocztowego może być uciążliwe.

Dużo lepszym rozwiązaniem jest wykorzystanie którejś z technik mnemotechnicznych. Dzięki nim można stworzyć długie, ale za to łatwiejsze do wprowadzenia hasła. Przykładowo mocne hasło może powstać z pierwszych liter trzech wersów fraszki Jana Kochanowskiego *Na matematyka*:

Ziemię **p**omierzył **i g**łębokie **m**orze,
Wie, **j**ako **w**stają **i z**achodzą **z**orze;
Wiatrom **r**ozumie, **p**raktykuje **k**omu

„ZpigmWjwizzWrpk”

Jeśli chcemy jeszcze bardziej zwiększyć siłę hasła, wystarczy dołożyć litery kolejnego wersu lub dokonać wymiany niektórych liter na cyfry i znaki specjalne (np. „i” na „!”, „z” na „2” itp.).

Jeszcze prostszą metodą jest sklejenie kilku słów wybranej sentencji i zastosowanie w nich drobnych przekształceń. O ile stosowanie haseł słownikowych jest niezalecane, o tyle hasło sklejone z wielu zmodyfikowanych słów, np. „Wystrzeg@jS!ęLudz!JednejKsiążk!”, jest już odporne na atak słownikowy.

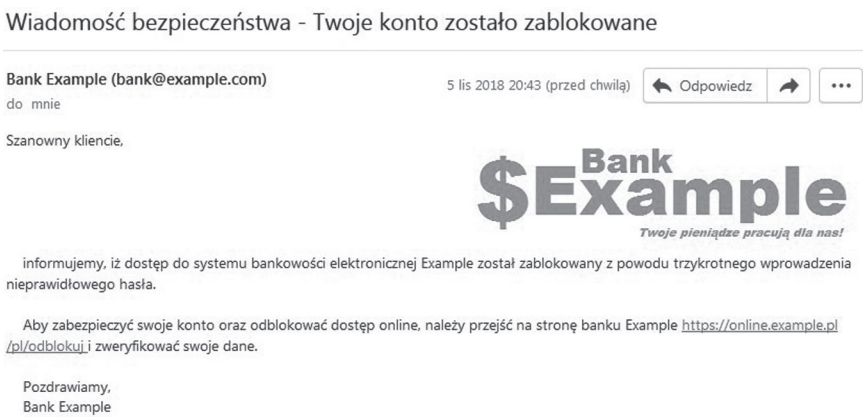
Metody przechwytywania haseł

Nawet najbardziej złożone hasło przestaje spełniać swoją funkcję, kiedy nie dbamy o jego poufność. Wielu użytkowników systemów komputerowych (zwłaszcza tych znajdujących się w sieci) nie zdaje sobie sprawy, jak często narażają swoje newralgiczne dane na przechwycenie.

Jedna z metod przechwytywania haseł opiera się na oprogramowaniu szpiegującym (ang. *spyware*). Są to programy monitorujące aktywność bez wiedzy użytkownika, w tym przyciskane klawisze (keyloggery). Do infekcji dochodzi najczęściej poprzez scam-maile. Są to wiadomości zachęcające do otwarcia zainfekowanych załączników. Urządzenie może także zostać zawirusowane poprzez wymienne nośniki pamięci (pendrive'y). Formą obrony przed tego rodzaju atakami jest nieotwieranie załączników od nieznanych nadawców, instalacja antywirusów skanujących zawartość urządzeń wymiennych oraz wykorzystywanie klawiatur ekranowych (rys. 1) do wpisywania szczególnie newralgicznych haseł, co uchroni nas, gdy w systemie znajduje się złośliwe oprogramowanie. Nie warto również logować się na komputerach w miejscach publicznych, nawet jeśli system operacyjny jest na bieżąco skanowany pod kątem złośliwego oprogramowania. Istnieją bowiem niewykrywalne keyloggery sprzętowe, które mogą być wbudowane w samą klawiaturę. Ponadto w przypadku nieszyfrowanego połączenia inni użytkownicy tego samego segmentu sieci mogą skutecznie przechwytywać przesyłane dane poprzez sniffery, czyli specjalne programy lub urządzenia, mogące monitorować dane przepływające w sieci.

Rys. 1. Wirtualna klawiatura zmniejsza ryzyko przechwycenia danych
Źródło: Opracowanie własne.

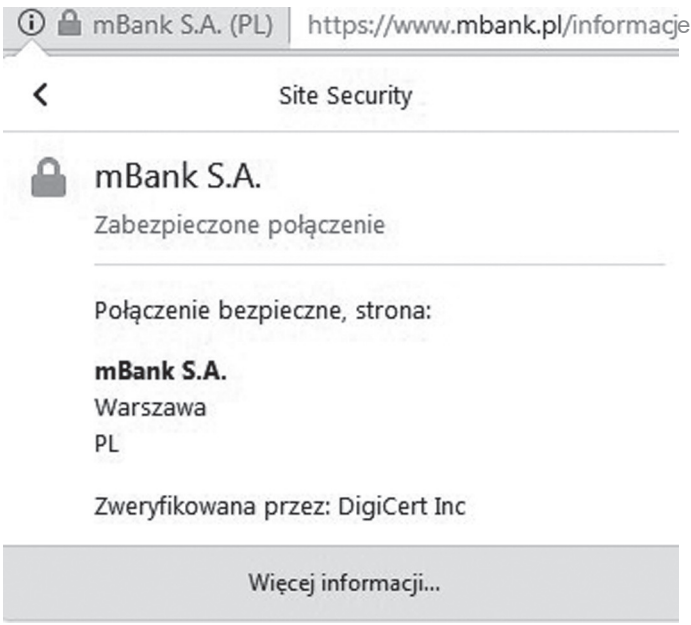
Inną popularną metodą przechwytywania haseł jest phishing. Metoda ta polega na wyłudzeniu danych od ofiary poprzez podszycie się pod zaufaną instytucję (np. bank) (*Phishing*, 2018). Wszystkie dane podane przez użytkownika na spreparowanej stronie są automatycznie przekazywane do przestępców. Na szczęście strony phishingowe można łatwo rozpoznać po nieprawidłowym adresie.



Rys. 2. Przykładowy mail phishingowy
Źródło: Opracowanie własne.

Przykładem bardziej wyrafinowanej metody przechwytywania newralgicznych danych jest pharming (zatrucie systemu nazw domenowych). Jeśli uda się doprowadzić do zapisu fałszywego skojarzenia domena – serwer w pamięci podręcznej systemu DNS, użytkownik, wchodząc na swoją zaufaną stronę, może zostać sprowadzony na stronę znajdującą się pod „opieką" atakującego. Dlatego przed każdym logowaniem na stronie internetowej warto sprawdzić, na kogo wystawiony jest certyfikat SSL / TLS (rys. 3). Należy pamiętać, że sama obecność zielonej kłódki nie gwarantuje bezpieczeństwa[5]. Szczególną czujność powinien wzbudzić komunikat przeglądarki o nieprawidłowo podpisanym certyfikacie.

[5] Takie działanie nie wymaga żadnych nakładów finansowych ze strony atakującego. Od 12 kwietnia 2016 r. instytut certyfikacji Let's Encrypt dostarcza użytkownikom darmowe certyfikaty szyfrowania (*Let's Encrypt*, 2016).



Rys. 3. Warto sprawdzać, na kogo wystawiony jest certyfikat

Źródło: Opracowanie własne.

Analiza zabezpieczeń systemów bankowości elektronicznej

Uzyskanie przez osobę niepowołaną kontroli nad kontem bankowym wiąże się najczęściej z utratą pieniędzy. W przypadku kradzieży danych identyfikacyjnych żadna instytucja nie zwróci nam środków za transakcje przeprowadzone do czasu zgłoszenia zdarzenia. Aby zniechęcić przestępców, powinno się stosować wyjątkowo skuteczne metody autoryzacji. Nie należy przy tym zapominać, że zbyt skomplikowana autoryzacja może być uciążliwa dla klientów.

Na potrzeby artykułu przeanalizowano systemy bankowości elektronicznej siedmiu największych banków na podstawie sprawozdań finansowych za I kwartał 2017 r. (*Raport*, 2017). W obliczeniach dla systemów, które wymagają użycia w haśle przynajmniej jednej litery, przyjęto, że użytkownik posługuje się alfabetem polskim. Wyjątkiem jest bank PKO BP – brak tu możliwości wykorzystywania polskich znaków diakrytycznych w haśle.

Tabela 2. Wartości entropii dla haseł zbudowanych z minimalnych dopuszczalnych zbiorów znaków w systemach bankowości elektronicznej

Bank	Minimalny zbiór znaków	Kombinacje	Entropia	Inne zabezpieczenia
PKO BP	7 cyfr i jedna litera (bez polskich znaków diakrytycznych)	$10^7 * 26$	27.95	Zabezpieczenie antyphishingowe
Bank Pekao	8 cyfr, mała i wielka litera	$10^8 * 32^2$	36.57	Maskowanie hasła, wirtualna klawiatura
BZ WBK	6 cyfr, mała i wielka litera	$10^6 * 32^2$	29.93	Maskowanie hasła, wirtualna klawiatura, zabezpieczenie antyphishingowe
mBank	7 cyfr i jedna litera	$10^7 * 32$	28.25	–
ING Bank Śląski	8 cyfr, mała i wielka litera	$10^8 * 32^2$	36.57	Maskowanie hasła
Bank BGŻ BNP Paribas	8 cyfr, mała i wielka litera	$10^8 * 32^2$	36.57	Maskowanie hasła, kody SMS, karta kryptograficzna
Bank Millennium	8 cyfr	10^8	26.57	Zabezpieczenie antyphishingowe, wirtualna klawiatura, maskowanie hasła*, podanie dwóch cyfr PESEL, numeru dowodu osobistego lub paszportu, wirtualna klawiatura

* Maskowany jest identyfikator (PESEL, numer dowodu osobistego lub paszportu)

Źródło: Opracowanie własne.

W żadnym z wymienionych banków nie jest możliwe użycie haseł krótszych niż 8 znaków. W Banku Pekao, ING Banku Śląskim oraz Banku BGŻ BNP Paribas minimalna długość tworzonych haseł to 10 znaków. Ponadto większość serwisów udostępnia dodatkowe zabezpieczenia antykradzieżowe. Przed phishingiem ostrzega spersonalizowany obrazek użytkownika, wyświetlający się w trakcie logowania. Zmniejsza to skuteczność wyłudzeń przy użyciu spreparowanych stron. Wirtualna klawiatura utrudnia pracę keyloggerom – kolejne znaki mogą zostać wybrane za pomocą myszki. W podobnym celu wykorzystuje się maskowanie hasła. Jest to mechanizm, dzięki któremu klient wprowadza tylko wybrane (wylosowane przez system) znaki – nawet jeśli zostaną one przechwycone, nie spowoduje to natychmiast ujawnienia całego hasła.

Rys. 4. Do logowania w Banku Pekao wymagane jest użycie co najmniej 10 znakowych haseł
Źródło: (*Bank Pekao*).

Popularny mBank nie udostępnia wirtualnej klawiatury ani nie wykorzystuje żadnych mechanizmów maskujących hasła. Brak także jakichkolwiek mechanizmów antyphishingowych. Nie dziwi zatem, że to właśnie do klientów tego banku często rozsyłane są fałszywe maile. Każdy średnio zaawansowany użytkownik może z łatwością spreparować stronę logowania, uruchomić ją na własnym serwerze i przechwycić hasło, wykorzystując roztargnienie mniej doświadczonych użytkowników. Co prawda, mBank na swoich stronach ostrzega klientów przed fałszywymi wiadomościami (*mBank*, 2015), nasuwa się jednak pytanie: czy nie lepiej byłoby wdrożyć proste zabezpieczenie w postaci obrazka przypisanego do konta, zamiast ostrzegać klientów przed konsekwencjami jego braku?

Na uwagę zasługują rozwiązania zastosowane w Banku Millennium. Hasło logowania składa się tutaj dokładnie z ośmiu cyfr, tym samym cechuje je najniższa entropia. Jednak do zalogowania się w systemie potrzebna jest także znajomość numeru PESEL, dowodu osobistego lub paszportu, co utrudnia niepowołanym osobom dostęp do konta. Ponadto bank ten jako jedyny zaimplementował wszystkie popularne zabezpieczenia przed przechwyceniem danych, takie jak spersonalizowana grafika wyświetlana podczas logowania, maskowanie identyfikatora oraz wirtualna klawiatura. Ten przykład pokazuje, że niewielka złożoność głównego hasła nie musi determinować bezpieczeństwa całego systemu.

Podsumowanie

Najsłabszym ogniwem wszystkich systemów zabezpieczeń jest człowiek. Niezależnie od ustaw, które, jak się wydaje, nie nadążają za postępem technologicznym, warto zachować zdrowy rozsądek i korzystać z niesłownikowych, unikatowych haseł o długości 12 znaków lub dłuższych. Warto także pamiętać, by nie wprowadzać haseł na nie swoim urządzeniu oraz dokonywać ich okresowych zmian. Uważajmy na złośliwe oprogramowanie – nie otwierajmy załączników od nieznanych nadawców maili, starajmy się też weryfikować autentyczność osób i instytucji, którym powierzamy nasze dane. Pozwoli to uniknąć wielu nieprzyjemnych sytuacji.

Literatura

ATI Radeon X850 XT Platinum AGP (2018). Pobrane z: https://videocardz.net/ati-radeon-x850-xt-platinum-agp/ (26.01.2018).

Bezpieczeństwo procesu logowania do nowego serwisu. Pobrane z: https://www.mbank.pl/pomoc/info/bezpieczenstwo/bezpieczenstwo-procesu-logowania-do-nowego-serwisu.html (14.03.0218).

Bezpieczne logowanie. Pobrane z: https://planet.bgzbnpparibas.pl/retail/static/help/0_EXBNP/Others.html (14.03.2018).

Consumer Password Worst Practices (2014). The Imperva Application Defense Center (ADC). Pobrane z https://www.imperva.com/docs/gated/WP_Consumer_Password_Worst_Practices.pdf (26.01.2018).

ING – Centrum pomocy. Pobrane z: https://www.ingbank.pl/indywidualni/bankowosc-internetowa/centrum-pomocy (14.03.2018).

e-skok. Pobrane z: https://e-skok.pl (29.01.2018).

Entropia. W: Encyklopedia PWN. Pobrane z: https://encyklopedia.pwn.pl/haslo/entropia; 4011112.html (14.03.2018)

Borda, M. (2011). Fundamentals in Information Theory and Coding (s. 11). Springer.

8x Nvidia GTX 1080 Hashcat Benchmarks (2018). Pobrane z: https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40 (29.01.2018).

Hasła, Obrazek Bezpieczeństwa i Certyfikaty. Pobrane z: https://www.pkobp.pl/bankowosc-elektroniczna/ipko/bezpieczna-bankowosc/hasla-obrazek-bezpieczenstwa-i-certyfikaty (14.03.2018).

Bank Pekao. Instrukcje Pekaobiznes24. Pobrane z: https://www.pekao.com.pl/mis/bankowosc_elektroniczna/instrukcje_pf24 (14.03.2018).

Let's Encrypt – Leaving Beta, New Sponsors (2016). Pobrane z: https://letsencrypt.org/2016/04/12/leaving-beta-new-sponsors.html (29.01.2018).

Mask Attack. Pobrane z: https://hashcat.net/wiki/doku.php?id=mask_attack (26.01.2018).

mBank ostrzega przed fałszywymi wiadomościami email dotyczącymi zablokowania rachunku (2015). Pobrane z: https://www.mbank.pl/informacje-dla-klienta/post,6147,mbank-ostrzega-przed-falszywymi-wiadomosciami-email-dotyczacymi-zablokowania-rachunku.html (29.01.2018).

NVIDIA Unveils GeForce GTX 1080 Ti: Available Week of March 5th for $699 (2017). Pobrane z: https://www.anandtech.com/show/11172/nvidia-unveils-geforce-gtx-1080-ti-next-week-699 (29.01.2018).

Phising (2018). W: *Wikipedia. The Free Encyclopedia*. Pobrane z: https://en.wikipedia.org/wiki/Phishing (29.01.2018).

Pomoc. Zmiana hasła. Pobrane z: https://planet.bgzbnpparibas.pl/retail/static/help/0_EXBNP/Others.html.

RainbowCrack Project – SHA1 Rainbow Tables (2017). Pobrane z: http://project-rainbowcrack.com/table.htm (29.01.2018).

Raport PRNews.pl: Aktywa banków – I kw. 2017 (2017). Pobrane z: https://prnews.pl/raport-prnews-pl-aktywa-bankow-i-kw-2017-360561 (29.11.2019).

Rozporządzenie 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 (2004). *Dziennik Ustaw Rzeczypospolitej Polskiej*, 100, poz. 1024.

Sposoby logowania do serwisu BZWBK24. Pobrane z: https://blog.bzwbk.pl/2014/05/logowanie_bzwbk24-2 (14.03.2018).

The Unicode Consortium, Unicode ® 10.0.0. Pobrane z: https://www.unicode.org/versions/Unicode10.0.0/ (26.01.2018).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (1997). *Dziennik Ustaw Rzeczypospolitej Polskiej*, 133, poz. 883.

Tekst w wersji poprawionej wpłynął do redakcji 17 marca 2018 r.

Wojciech Balawender
A first-year student of MA IT studies
The Department of IT Studies and the Science of Materials
The Students' Scholarly Circle of Infologists
The Institute of Library Science and Scientific Information
University of Silesia in Katowice
e-mail: wbalawen@us.edu.pl

The strength of passwords in the context of the protection of collections of data

Abstract: The article is devoted to the comparison of the quality of entries by means of information entropy. One itemised the key legal regulations which the administrators of databases must follow. One presented certain methods of intercepting and breaking passwords and emphasised the fundamental principles of safety, which should be followed by each computer user, including the mnemonic methods of creating strong passwords. One conducted an analysis of the security systems of identification-related processes of seven major banks.

Keywords: Database. PUODO. RODO. The strength of a password