ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2015
Seria: ORGANIZACJA I ZARZĄDZANIE z. 86 Nr kol. 1946

Artur SZLESZYŃSKI
Wyższa Szkoła Oficerska Wojsk Lądowych
im. gen. T. Kościuszki Wrocław
Instytut Dowodzenia
a.szleszynski@wso.wroc.pl

ZARZĄDZANIE POUFNOŚCIĄ ZASOBÓW INFORMACYJNYCH W SYSTEMACH TELEINFORMATYCZNYCH

Streszczenie. W artykule przedstawiono skuteczność ochrony treści pliku za pomocą hasła. Treść związana jest z atrybutem poufności zasobu informacyjnego. W pracy przyjęto następujące kryterium oceny hasło powinno być tak skonstruowane, żeby czas dotarcia do treści pliku wynosił co najmniej 2 godz. i żadne z użytych w badaniu haseł nie spełniło wymogów zawartych w kryterium oceny.

Słowa kluczowe: atrybut poufności zasobu informacyjnego, ochrona hasłem.

CONFIDENTIALITY OF INFORMATION RESOURCES MANAGEMENT IN ICT SYSTEMS

Summary. In the paper the protective efficacy contents of the file with a password is presented. The content is related to the confidentiality attribute of information resource. In this work, the following criterion password should be designed so that the time to reach the contents of the file is at least 2 hours. None of the terms used in the study did not meet the requirements of the criterion.

Keywords: confidentiality attribute information resource, password protection.

1. Geneza problemu

Zasób informacyjny, którego fizyczną reprezentacją w systemie teleinformatycznym jest plik, stanowi ważny element organizacji. Proces zarządzania bezpieczeństwem polega na utrzymaniu niezmienionych atrybutów bezpieczeństwa zasobów informacyjnych i rozpoczyna się od wskazania informacji wrażliwych. Wskazanie informacji wrażliwych oraz miejsc ich

powstawania i dystrybucji jest istotne dla sprawnej realizacji procesu ochrony. Działanie to wynika z faktu, że nie jest możliwa ochrona wszystkich zasobów informacyjnych powstających i wykorzystywanych w organizacji. Zatem należy wybrać te z zasobów, których utrata lub uszkodzenie może wprowadzić największe zakłócenia w funkcjonowaniu organizacji. Zasoby te klasyfikowane są jako wrażliwe zasoby informacyjne podmiotu.

Zarządzanie bezpieczeństwem informacji w organizacji, zgodnie z normą ISO-IEC 27001, jest procesem. Obejmuje on cztery główne podprocesy takie, jak: planowanie działań, wdrażanie planowanych działań, sprawdzenie uzyskanych wyników oraz działania korygujące [7]. Elementem procesu zarządzania bezpieczeństwem zasobów informacyjnych są regularnie wykonywane pomiary. Zawierają się one w czynnościach sprawdzających, a ich celem jest wykrywanie naruszeń atrybutów bezpieczeństwa zasobów informacyjnych oraz powiązanych incydentów w bezpieczeństwie. Z każdym incydentem w bezpieczeństwie związana jest podatność, która jeśli zostanie wykorzystana, będzie wpływać na bezpieczeństwo zgromadzonych zasobów informacyjnych [1, 8].

Pomiary, wykonywane na podstawie analizy ryzyka, mają wskazać, które z zasobów informacyjnych mogą być zagrożone. Łącząc wyniki pomiarów z analizą ryzyka możliwe jest oszacowanie skutków naruszenia atrybutów bezpieczeństwa zasobów informacyjnych, które są najbardziej zagrożone przez incydenty w bezpieczeństwie. W artykule przedstawiono wybrane metody ochrony treści zasobów informacyjnych stosowane w pakietach biurowych. Wybór pakietów biurowych wynika z faktu ich częstego wykorzystywania do tworzenia plików wewnątrz organizacji. Jedną z metod ochrony treści pliku przed nieuprawnionym zapoznaniem się z nią jest ochrona przed jego otwarciem, wykonywana za pomocą hasła. W badaniach opisanych w literaturze wykazano istnienie związku pomiędzy strukturą i długością hasła a czasem potrzebnym do jego złamania. Opisano metodę szacowania zmian atrybutu poufności zasobu informacyjnego poddanego oddziaływaniu incydentu w bezpieczeństwie.

2. Identyfikacja problemu

Zarządzanie bezpieczeństwem zasobów informacyjnych wymaga opracowania i skoordynowania działań wewnątrz organizacji. Za ten element wewnętrzny odpowiada zespół zarządzania bezpieczeństwem informacyjnym organizacji. Ponieważ jest mowa o zarządzaniu bezpieczeństwem można zadać pytanie - jak motywować bezpieczeństwo?, więc gdyż pojęcie to odnosi się do subiektywnego poczucia braku zagrożenia lub zagrożeń dla danego zasobu. Oczywiste jest, że nie jest to możliwe. Dlatego w literaturze przedmiotu pojęcie bezpieczeństwa zasobów informacyjnych odnoszone jest do atrybutów, opisujących stan zasobu [1, 6, 9].

Normy zalecają posługiwanie się cyklem Deminga do podnoszenia lub utrzymania przyjętego poziomu bezpieczeństwa [7]. Cykl ten, nazywany również procesem, wymaga skoordynowania większej lub mniejszej liczby zadań. Liczbę zadań oraz zakres determinują pomiary wskazujące, w jakim stopniu obecna sytuacja odbiega od stanu oczekiwanego. Pierwszym pytaniem, które może się pojawić, jest – jak zmierzyć wartości atrybutów bezpieczeństwa zasobów informacyjnych? Przykład odpowiedzi na tak sformułowane pytanie przedstawiono w literaturze przedmiotu [6, 8, 9], określając wartość wyjściową atrybutów przy użyciu wartości liczbowej. Podejście to zakłada, że w momencie rozpoczęcia pomiaru każdy oceniany zasób ma niezmienione wartości liczbowe dla każdego z atrybutów [8, 9]. Analizując zmiany zidentyfikowane w zasobach informacyjnych, szacując ich rozmiar można określić proporcjonalną zmianę wartości każdego z atrybutów bezpieczeństwa. Wynikiem pomiarów powinny być wnioski i zalecenia dotyczące utrzymania poziomu bezpieczeństwa zasobów informacyjnych lub zbiór zadań kończących się osiągnięciem celu, jakim jest oczekiwany poziom bezpieczeństwa zasobów informacyjnych przy utrzymaniu założonego czasu i budżetu.

Jednym z zadań chroniących atrybut poufności zasobów informacyjnych jest ochrona plików wytwarzanych za pomocą pakietów biurowych. Pakiety te oferują funkcje chroniące pliki przed dostępem osób nieuprawnionych.

Obecnie wymiana informacji pomiędzy różnymi podmiotami realizowana jest za pomocą sieci teleinformatycznych. Część wymienianych plików będą stanowiły dokumenty utworzone za pomocą pakietów biurowych. Pomiędzy jednostkami administracji rządowej wymieniane są informacje o różnym stopniu wrażliwości. Interesujące jest poznanie odpowiedzi na pytanie, jak administracja rządowa przygotowana jest do radzenia sobie z cyberatakami.

Wyniki kontroli przeprowadzonej przez Najwyższą Izbę Kontroli pokazały, że w administracji szczebla centralnego kwestia zarządzania bezpieczeństwem informacyjnym oraz odporności na ataki z sieci Internet jest nieodpowiednia [4]. Raport informuje, że kontrolowane ministerstwa nie koordynowały działań z obszaru bezpieczeństwa teleinformatycznego między sobą. Można zadać pytanie – w jaki sposób chronione będą dane obywateli przetwarzane przez systemy teleinformatyczne, wchodzące w skład e-administracji? W tym zestawieniu najlepiej oceniono Ministerstwo Obrony Narodowej, Agencję Bezpieczeństwa Wewnętrznego oraz Naukową Akademicką Sieć Komputerową. Wskazano, że wymienione instytucje mają najlepiej przygotowane zespoły reagowania do radzenia sobie z cyberatakami [4].

Problemem badawczym, który zamierza się rozwiązać w artykule, jest udzielenie odpowiedzi na pytania:

- jak skuteczna jest ochrona treści plików przed nieuprawnionym dostępem w pakiecie biurowym, w zależności od struktury i długości przyjętego hasła?

- Jakie inne metody, ochrony treści plików można wdrożyć w celu osiągnięcia założonego poziomu ochrony przed nieuprawnionym dostępem?

Jako kryterium do oceny skuteczności ochrony treści pliku przed nieautoryzowanym otwarciem przyjęto czas potrzebny programowi łamiącemu hasła do jego znalezienia. Jako krytyczną wartość czasu przyjęto 2 godz. (7200 s). Kryterium to wynika z faktu, że czas ten jest na tyle długi, że większość atakujących może się zniechęcić do podejmowania prób dotarcia do treści źródłowej chronionych plików. Kolejnym założeniem przyjętym w artykule jest posługiwanie się przez atakującego standardowo dostępnym oprogramowaniem i sprzętem komputerowym. Przez pojęcie standardowo dostępnego oprogramowania rozumie się programy dostępne w sieci Internet, np. Office Password Unlocker. Przez standardowo dostępny sprzęt rozumie się powszechnie dostępne komputery, a nie urządzenia specjalistyczne, przeznaczone do łamania zabezpieczeń kryptograficznych. Zatem atakujący nie powinien posługiwać się specjalistycznym oprogramowaniem oraz komputerem lub komputerami zdolnymi realizować równoległe przeszukiwanie zbioru możliwych haseł. Komputery wykorzystujące technikę obliczeń równoległych wykorzystują wysokowydajne procesory graficzne.

3. Propozycja rozwiązania

Zawartość plików przechowujących informacje wrażliwe chroni się przy użyciu metod kryptograficznych. W zależności od złożoności zastosowanej metody kryptograficznej, użytego w niej klucza szyfrującego czas dotarcia do treści pliku ulega wydłużeniu lub skróceniu. Chcąc ustalić czy dana metoda kryptograficzna skutecznie chroni zasób informacyjny, należy założyć minimalny czas potrzebny do dotarcia do zawartości pliku przez osobę nieuprawnioną. W opisanym badaniu przyjęto czas krytyczny 2 godz. Czas ten wzięto z pracy A. Szleszyńskiego i A. Wojaczek, gdzie na podstawie danych z portali specjalistycznych wyznaczono minimalny czas dotarcia do treści pliku [10]. Następnie wykorzystano mechanizm ochrony treści pliku przy użyciu hasła chroniącego plik przed otwarciem przez nieuprawnioną osobę. W badaniu przyjęto różne warianty haseł, będące kombinacjami samych liter, samych cyfr oraz liter i cyfr. Długości haseł przyjęto od 3 do 5 znaków, ponieważ są one łatwe do zapamiętania przez osoby posługujące się nimi. Dla opisanego rozwiązania program znajdujący hasło musiał przeszukać przestrzeń od 1000 (dla hasła, składającego się z trzech cyfr) do 60466176 (dla hasła o długości pięciu znaków, składającego się z cyfr i liter) możliwych realizacji haseł. Liczba możliwych kombinacji wyznaczana jest na podstawie zależności (1):

$$S = L^n, \tag{1}$$

gdzie: S – liczba możliwych kombinacji haseł, L – liczba znaków, które można użyć do utworzenia, n – liczba znaków w haśle.

Stosowana w pakiecie biurowym ochrona przed otwarciem pliku polega na zaszyfrowaniu jego treści, fragmenty dotyczące organizacji pliku pozostają zaś niezmienione; co pokazują wyniki pomiarów współczynnika liczby zmienionych bajtów w chronionym pliku (dbm) w stosunku do pliku źródłowego[1]. Liczbę zmienionych bajtów oraz wartość współczynnika dbm pokazano w tabeli 1. Sposób wyznaczania wartości współczynnika liczby zmienionych bajtów opisano w publikacji A. Szleszyńskiego [9]. Metoda wykorzystuje zalecenia norm ISO/IEC 27004:2009 oraz NIST 800-55 [3,5].

Pierwsze trzy pozycje zajmują hasła składające się z pięciu znaków, ale na czwartej pozycji jest hasło składające się z trzech znaków. Zatem próba znalezienia hasła tylko na podstawie liczby zmienionych bajtów jest bezcelowa, gdyż (co pokazano na rysunku 1), hasło składające się z małej liczby znaków spowodowało powstanie dużej liczby zmienionych bajtów w pliku. Atakujący chcąc posłużyć się tą metodą szacowania długości hasła musi dysponować plikiem wzorcowym, w celu wyznaczenia wartości współczynnika dbm. Plik wzorcowy zawiera niezabezpieczoną informację. Dodatkowo hasła składające się z czterech lub pięciu znaków spowodowały mniejsze zmiany ilościowe niż hasła składające się z mniejszej liczby znaków.

Z danych umieszczonych w tabeli 1 wynika, że znalezienie struktury hasła chroniącego plik na podstawie liczby zmienionych bajtów jest trudne.

Dla próby badawczej (pokazanej w tabeli 1) wyznaczono parametry statystyki, opisującej zmienność współczynnika dbm (tabela 2). Rozrzut próby jest nieduży i wynosi 0,00105, co stanowi 0,21% minimalnej i maksymalnej wartości dbm wyznaczonych dla próby badawczej.

Tabela 1

Parametry plików chronionych przed otwarciem za pomocą hasła

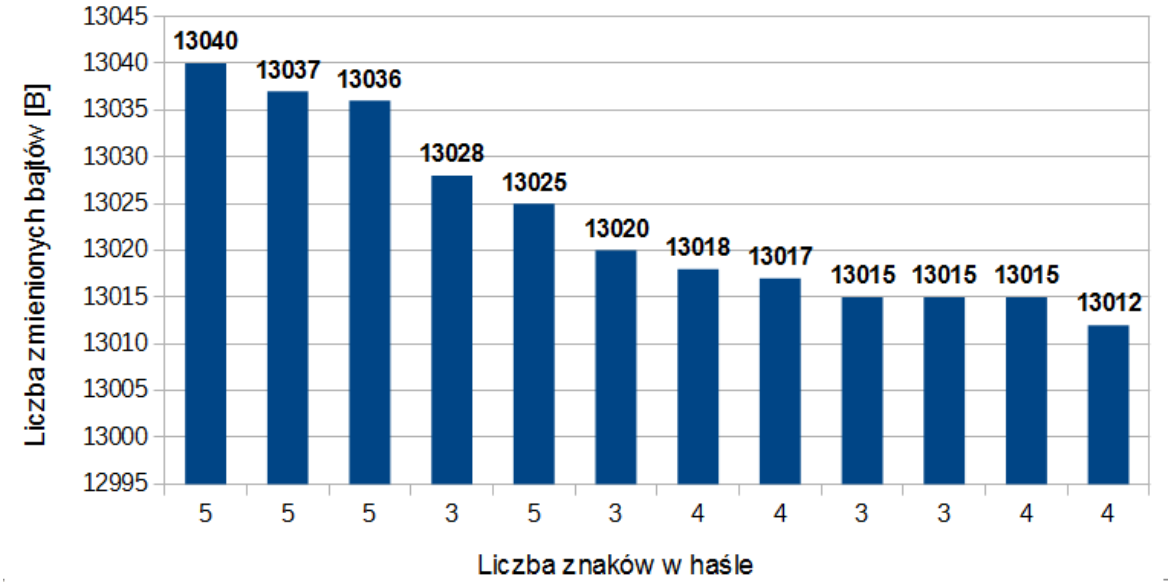
Lp.	Liczba zmienionych bajtów w chronionym pliku [B]	Wartość dbm	Hasło
1.	13040	0,48978	12345
2.	13037	0,48967	abcde
3.	13036	0,48963	1b3d5
4.	13028	0,48933	123

[1] Przez plik źródłowy rozumie się plik niechroniony hasłem.

cd. tabeli 1

5.	13025	0,48922	a2c4d
6.	13020	0,48903	1b3
7.	13018	0,48896	abcd
8.	13017	0,48892	a2c4
9.	13015	0,48884	abc
10.	13015	0,48884	a2c
11.	13015	0,48884	1234
12.	13012	0,48873	1b3d

Źródło: opracowanie własne.



Rys. 1. Związek między długością hasła a liczbą zmienionych bajtów w chronionym pliku
Fig. 1. Relation between password length and number of changed bytes in protected file
Źródło: opracowanie własne.

Tabela 2

Parametry statystyki opisowej współczynnika dbm, wyznaczone dla próby testowej

Parametr	**Wartość**
Średnia	0,48915
Mediana	0,48899
Dominanta	0,48884
Odchylenie standardowe	0,00037
Wariancja próbki	$1{,}36673*10^{-70}$
Minimum	0,48873
Maksimum	0,48978

Źródło: opracowanie własne.

W wyniku zastosowania opisanego mechanizmu ochrony rozmiar zmodyfikowanego pliku wzrósł o 512 B (plik wzorcowy miał rozmiar 26624 B, a pliki chronione przed otwarciem miały rozmiar 27136 B).

Dla próby testowej zbadano czas, jaki był potrzebny programowi łamiącemu hasło do jego znalezienia. W tym celu wykorzystano wersję demonstracyjną programu Office Password Unlocker. Program był w pełni funkcjonalny, jedynym ograniczeniem był 30-dniowy okres jego użytkowania. Dla potrzeb eksperymentu wykonano 12 plików, każdy zabezpieczony innym hasłem. Listę haseł użytych w badaniu oraz ich strukturę pokazano w tabeli 3.

W przypadku 3-znakowych haseł ochrona treści pliku nie istnieje. Czas 1 s potrzebny do jego odnalezienia jest 7200 razy krótszy od założonego na wstępie. Z danych zamieszczonych w tabeli 3 wynika, że dopiero hasła składające się z pięciu znaków zbliżają się do wartości granicznej. Bardzo niska jest skuteczność haseł składających się z samych liter. Czas potrzebny do złamania takiego hasła jest krótszy niż 3 minuty. Jest to istotne, ponieważ hasła te są najłatwiejsze do zapamiętania przez użytkownika.

Badanie potwierdziło dane umieszczone w literaturze przedmiotu, że efektywny poziom ochrony gwarantują hasła o długości co najmniej siedmiu znaków. Hasła te są trudne do zapamiętania, więc użytkownicy mogą je zapisywać w plikach lub umieszczać w innych miejscach, np. pod klawiaturą lub na obudowie monitora.

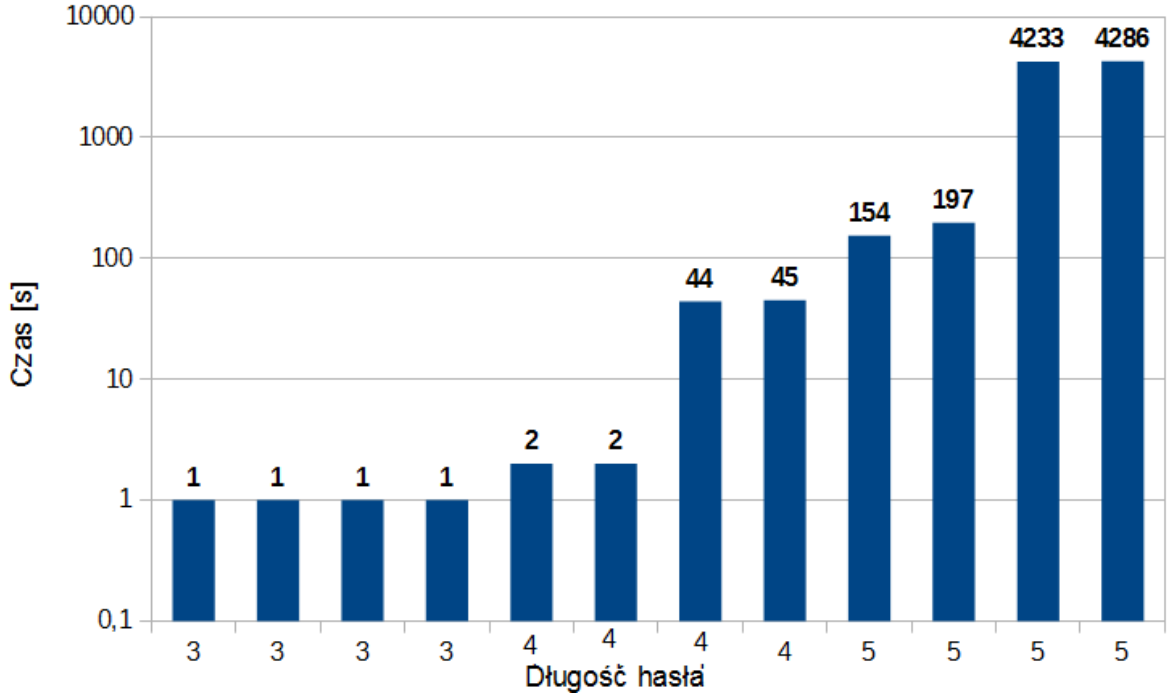
Tabela 3

Czas potrzebny do odnalezienia hasła chroniącego treść pliku

Czas znajdowania hasła przez program testowy [s]	**Hasło**	**Typ znaków użytych w haśle**	**Liczba znaków w haśle**
1	123	cyfry	3
1	1b3	cyfry-litery	3
1	abc	litery	3
1	a2c	litery-cyfry	3
2	abcd	litery	4
2	a2c4	litery-cyfry	4
44	1b3d	cyfry-litery	4
45	1234	cyfry	4
154	abcde	litery	5
197	a2c4d	litery-cyfry	5
4233	1b3d5	cyfry-litery	5
4286	12345	cyfry	5

Źródło: opracowanie własne.

W badaniu przyjęto maksymalną długość hasła, wynoszącą pięć znaków. Wybór ten wynikał z faktu, iż hasło takie jest łatwe do zapamiętanie i nie będzie wymagało jego zapisywania. Jednakże chcąc efektywnie zarządzać bezpieczeństwem zasobów informacyjnych, należy znaleźć punkt siodłowy pomiędzy strukturą i długością hasła a możliwością jego zapamiętania. Hasło trudne do do złamania jest trudne do zapamiętania. Pakiety biurowe (komercyjne i dystrybuowane na licencji OpenSource) oferują inne mechanizmy chroniące pliki. Metoda ta polega na zaszyfrowaniu całego pliku, a nie wybranych fragmentów. Interesująca stała się próba znalezienia odpowiedzi na pytanie czy istnieje oprogramowanie mogące złamać zmodyfikowane zabezpieczenia – zabezpieczenia trudniejsze do złamania? Autor podjął próbę znalezienia w sieci Internet oprogramowania, które zajmuje się łamaniem plików kryptograficznie, zabezpieczonych za pomocą krypto-systemów, np. 3DES czy AES.



Rys. 2. Czas potrzebny programowi testowemu do złamania hasła w zależności od jego długości
Fig. 2. Time consume by test software to password break down depend password length
Źródło: opracowanie własne.

Nie udało się znaleźć tego typu oprogramowania. Nie jest ono powszechnie dostępne, ponieważ stanowi narzędzie laboratoriów kryptoanalitycznych. Prawdopodobnie posługiwanie się nim nie polega na dotarciu do postaci źródłowej zaszyfrowanego pliku, a jedynie na wskazaniu struktury klucza deszyfrującego. Dotarcie do podanej struktury jest złożone obliczeniowo, co wynika z konieczności analizowania dużej liczby możliwych kombinacji. Dla przykładu dla kryptosystemu AES o długości klucza szyfrujące 256 bitów

jest to $8x10^{37}$ kombinacji. Taka liczba możliwych kombinacji sprawia, że złamanie zabezpieczenia możliwe jest tylko dla instytucji dysponujących komputerami o dużej mocy obliczeniowej [2].

Dla zespołów odpowiedzialnych za zarządzanie bezpieczeństwem informacji w organizacji problem z możliwym odzyskaniem zawartości pliku (plików) jest zadaniem do rozwiązania. Po pierwsze, należy zadbać o właściwe szkolenie użytkowników, którzy są osobami odpowiedzialnymi za powierzone im pliki. Kolejnym działaniem jest system bezpiecznego przechowywania kluczy deszyfrujących. Jest to istotne, ponieważ w organizacji, która dysponuje dużymi zbiorami plików szyfrowanie pojedynczych plików jest bezcelowe. Efektywniejszym rozwiązaniem jest szyfrowanie partycji dyskowych, co uniemożliwia korzystanie z zasobów osobom postronnym. Bezpieczne przechowywanie kluczy do deszyfracji plików jest konieczne do odzyskania danych po awarii sprzętu.

W mniejszych organizacjach szyfrowanie pojedynczych plików może być stosowane do czasu wprowadzenia jednolitego rozwiązania, dotyczącego kryptograficznej ochrony zasobów. Wadą indywidualnego szyfrowania jest brak zarządzania kluczami do szyfrowania i deszyfrowania plików. Obowiązek ten cedowany jest na użytkowników, którzy nie zawsze rozumieją sens i cel takich działań. Konieczne jest szkolenie dotyczące sposobu tworzenia haseł oraz zasad ich bezpiecznego składowania i przesyłania. Można posłużyć się bardziej zaawansowanymi narzędziami do ochrony kryptograficznej. Jednak posługiwanie się metodami kryptograficznymi trudnymi do złamania może doprowadzić do sytuacji, gdy w wyniku niewłaściwego zarządzania kluczami dotarcie do treści pliku będzie niemożliwe.

Utrzymanie atrybutu poufności wrażliwych zasobów informacyjnych nie jest jedynym zadaniem zespołu odpowiedzialnego za utrzymanie bezpieczeństwa informacyjnego wewnątrz organizacji. Należy kontrolować zmiany pozostałych atrybutów bezpieczeństwa wrażliwych zasobów bezpieczeństwa. Techniki pomiaru zmian atrybutów bezpieczeństwa opisano w pracach W. Rybickiego i A. Szleszyńskiego [8, 9].

Dopiero na podstawie tak wykonanych zadań należy przystąpić do opracowania harmonogramu prac oraz kosztorysowania projektu, którego celem będzie usunięcie stwierdzonych różnic pomiędzy stanami rzeczywistym a oczekiwanym. Koszt projektu zależy od zadań, jakie należy wykonać, ponieważ do każdego z zadania należy przydzielić określone zasoby. Koszt realizacji zadań wzrasta w momencie, kiedy do jego wykonania niezbędne są usługi specjalistyczne, wykonywane przez firmy zewnętrzne. Korzystanie z usług firm zewnętrznych podnosi ryzyko dla realizacji projektu. Podniesienie poziomu ryzyka wynika z możliwości niewywiązania się firmy z zamówionego zadania.

Koszt każdego zadania w projekcie obliczany jest na podstawie zależności (2). Na koszt ten składają się nakłady osobowe, zasoby materiałowe, użyte w zadaniu oraz koszty związane ze szkoleniami personelu lub usługami transportowymi (pocztowymi).

$$K_i = Z_o \cdot K_o + Z_m \cdot K_m + Z_u \cdot K_u, \quad (2)$$

gdzie: K_i – koszt i-tego zadania w projekcie, Z_o – liczba osób realizujących i-te zadanie w projekcie, K_o – koszty pracy osób wykonujących zadanie, Z_m – liczba zasobów materiałowych wykorzystanych w i-tym zadaniu, K_m – koszt zasobów materiałowych użytych w zadaniu, Z_u – liczba usług zastosowanych w zadaniu, K_u – koszt usług użytych w zadaniu.

Całkowity koszt projektu (K_p) obliczany jest jako suma kosztów wszystkich zadań cząstkowych wykonywanych w projekcie, co przedstawia zależność (3):

$$K_p = \sum_{i=1}^{n} K_i \quad (3)$$

Ryzyko w projekcie związane jest nie tylko z aspektem finansowym. Innym czynnikiem wpływającym na możliwość wystąpienia zdarzenia, jakim jest nieukończenie projektu jest przekroczenie czasu jego realizacji. Przekroczenie czasu przewidzianego w harmonogramie może wynikać z pominięcia w harmonogramie projektu zadań, które wpływają na osiągnięcie zamierzonych celów projektu. To zaś przekłada się na jakość projektu. Wydłużenie czasu realizacji zadań będzie skutkowało wzrostem kosztów, co nie jest jednoznaczne z gwarancją poprawy jakości prowadzonego projektu.

4. Podsumowanie

W artykule opisano skuteczność ochrony zawartości plików chronionych za pomocą haseł. Rozważania ograniczono do grupy plików wykonanych przy użyciu pakietów biurowych. Ograniczenie to wynikało z faktu, iż wiele dokumentów w typowej działalności organizacji wykonywanych jest przy użyciu oprogramowania biurowego.

Na podstawie wyników przeprowadzonego eksperymentu można stwierdzić, że hasła o długości do pięciu znaków nie wypełniły wymogu postawionemu w kryterium oceny. Czas potrzebny do złamania haseł chroniących treść plików był krótszy niż 2 godz.

Oznacza to, że hasła te pomimo swojej prostoty nie gwarantują należytej ochrony treści zasobu informacyjnego. Skoro treść nie jest chroniona, to nie zostanie zachowany atrybut poufności zasobu informacyjnego. Wyniki badań potwierdzają słuszność wymagania, dotyczącego ochrony danych osobowych przetwarzanych w systemie teleinformatycznym. W rozporządzeniu do Ustawy o ochronie danych osobowych wymaga się, aby pliki z danymi osobowymi były chronione hasłem składającym się z co najmniej ośmiu znaków. Czas potrzebny na odnalezienie hasła chroniącego plik wynosi od 58 godz. (same litery alfabetu łacińskiego) do 7 lat (kombinacja liter alfabetu łacińskiego i cyfr) [10].

Bibliografia

1. Białas A.: Bezpieczeństwo informacji i usług we współczesnej firmie lub organizacji, WNT, Warszawa 2006.
2. Bogdanov A., Kohvratovich D., Rechberger C., Biclique Cryptoanalysis of the Full AES, [dostęp on-line 1.09.2015] http://eprint.iacr.org/2011/449.pdf.
3. Chew E., Swanson M., Stine K., Bartol N., Brown A., Robinson W.: NIST Special Publication 800-55 Revision 1. Performance Measurement Guide for Information Security, National Institute of Standards and Technology, U.S. Department of Commerce, Computer Division, Gaithersburg, MD 20899-8930, 2008.
4. Informacja o wynikach kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, Najwyższa Izba Kontroli, Warszawa 2015.
5. ISO/IEC 27004:2009 Information technology – Security techniques – Information security management – Measurement.
6. Jóźwiak I.J., Szleszyński A.: Study of the security of processes running in computer operating,in: Safety and Reliability: methodology and applications: proceedings of the [XXIV] European Safety and Reliability Conference ESREL 2014/ed. Tomasz Nowakowski [i in.] Taylor & Francis Group, 2015, pp. 651-654.
7. PN ISO/IEC 27001 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2014.
8. Rybicki W., Szleszyński A.: Zarządzanie poziomem bezpieczeństwa informacyjnego w systemach teleinformatycznych. Etap I. Metody pomiaru bezpieczeństwa zasobów informacyjnych w systemach teleinformatycznych, Praca naukowo – badawcza, WSOWL, Wrocław 2014.
9. Szleszyński A.: Pomiar bezpieczeństwa informacji w zarządzaniu bezpieczeństwem w systemie teleinformatycznym, Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i Zarządzanie, z. 74, Gliwice 2014.
10. Szleszyński A., Wojaczek A.: Bezpieczeństwo zasobów informacyjnych chronionych przy pomocy haseł. Zeszyty Naukowe WSOWL, Wrocław 2015 (w przygotowaniu).

Abstract

The paper shows the effectiveness of content protection files with passwords. As an object of study selected files created using MS Office. To protect the content used passwords that are shown in Table 1. The study showed that the number of bytes changed in the encrypted file is not dependent on the password length (Fig.1). Using the Office Password Unlocker made

attempts to break down the passwords. None of the adopted base on passwords do not take time longer than 2 hours his break. Short 3-character passwords program was break down in less than 1 second time. This means that passwords do not provide any protection contents of the file.