Karol KRÓL
Uniwersytet Rolniczy w Krakowie
Wydział Inżynierii Środowiska i Geodezji
Katedra Gospodarki Przestrzennej i Architektury Krajobrazu

ORGANIZACYJNE ASPEKTY ZARZĄDZANIA BEZPIECZEŃSTWEM DANYCH Z PERSPEKTYWY ZAGROŻEŃ PHISHINGU

Streszczenie. Wraz z rozwojem i dostępnością Internetu obserwuje się wzrost aktywności przestępczej w sieci. Próby wyłudzenia informacji strategicznych oraz danych osobowych są coraz częstsze. Stanowi to wyzwanie nie tylko dla indywidualnych użytkowników, ale również dla kadry zarządzającej personelem przedsiębiorstw. Celem pracy jest przedstawienie mechanizmu oszustwa internetowego typu „*spear phishing*", polegającego na próbie wyłudzenia danych autoryzacji dostępu do internetowych kont prywatnych lub służbowych. W pracy przedstawiono założenia niskonakładowego, uniwersalnego audytu wewnętrznego, który w sposób kontrolowany pozwoliłby na sondaż stopnia wyszkolenia i podatności pracowników na próby wyłudzenia poufnych danych.

Słowa kluczowe: wyłudzanie informacji, bezpieczeństwo danych, audyt

SECURITY MANAGEMENT – PHISHING, THE CONCEPT OF AUDIT

Summary. Each month, more attacks are launched for the purpose of stealing account information, logon credentials, and identity information in general. This attack method known as phishing is most commonly initiated by sending out emails with links to spoofed websites that harvest information. This is a challenge not only for individual users but also for personnel management of enterprises. The aim of the study is to present the mechanism of spear phishing, which is one of the type of phishing attack. The paper presents the assumptions of universal audit of data security and information technology systems.

Keywords: spear phishing, data security, audit

1. Wprowadzenie oraz cel pracy

Nowoczesne technologie informacyjne odgrywają coraz większą rolę w kształtowaniu społeczeństwa informacyjnego[1], społeczeństwa sieci[2]. Internet pełni coraz więcej funkcji w życiu codziennym, a grono jego użytkowników stale rośnie.

Według badań Centrum Badania Opinii Społecznej[3] użytkownicy Internetu stanowią w Polsce ponad połowę ogółu dorosłych. W ciągu ostatnich sześciu lat konsekwentnie rośnie popularność zakupów dokonywanych w sieci. Towarzyszy mu wzrost zainteresowania mediami społecznościowym, telewizją internetową oraz innymi materiałami wideo. Ponadto nieustannie przybywa w Polsce użytkowników internetowych usług bankowych oraz czytelników cyfrowej prasy.

Wraz z rozwojem i dostępnością Internetu promowana jest idea bezpieczeństwa, wygody użytkowania oraz mnogości udogodnień, jakie niesie dostęp do sieci. Równie mocno podkreślane są potencjalne zagrożenia, które mu towarzyszą. W ostatnich latach obserwuje się wzrost aktywności przestępczej w sieci. Przyjmuje ona wiele form, które różnią się od siebie techniką, zasięgiem oddziaływania, wyrafinowaniem oraz wieloma innymi cechami, które wpływają na stopień zagrożenia dla użytkowników[4].

Liczba kont i haseł dostępu związanych z szeroką gamą usług świadczonych za pośrednictwem sieci stale rośnie. Przeciętny użytkownik Internetu posiada co najmniej kilka różnorakich internetowych kont prywatnych oraz konta służbowe, służące m.in. do transakcji finansowych, wymiany informacji, publicystyki lub rozrywki oraz wykonywania specjalistycznych czynności zawodowych. Każde z nich chronione jest loginem oraz hasłem dostępu. Często również wymaga uwierzytelnionego połączenia.

Wszystkie zabezpieczenia związane z autoryzacją dostępu można próbować ominąć z wykorzystaniem ataków typu phishing. Analitycy przewidują, że w nadchodzących latach spodziewana jest nowa fala ataków na urządzenia przenośne z dostępem do Internetu, w tym telefony, tablety i notebooki oraz sieci komputerowe, zwłaszcza korporacyjne i podmiotów strategicznych[5]. Ponadto obserwowany jest wzrost liczby ataków wykorzystujących techniki inżynierii społecznej, których celem jest uzyskanie dostępu do prywatnych danych, w tym haseł dostępu do skrzynek pocztowych, służbowych dokumentów, czy też uzyskanie możliwości połączenia z firmowymi aplikacjami, bazami danych lub infrastrukturą sieciową.

[1] Babik W.: Ekologia informacji – wyzwanie XXI wieku. „Praktyka i Teoria Informacji Naukowej i Technicznej", nr (1)37, 2002, s. 2.
[2] Castells M.: The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I. Malden, MA; Oxford, UK: Blackwell 2009, p. 10.
[3] CBOS: Internauci 2014. Centrum Badania Opinii Społecznej, Warszawa 2014, nr 82, s. 2-4.
[4] Wall D.S.: Cybercrime: The Transformation of Crime in the Information Age. Polity Press, Cambridge UK, 2007.
[5] Provos N., Rajab M. A., Mavrommatis P.: Cybercrime 2.0: when the cloud turns dark. „Communications of the ACM", No. 52(4), 2009, p. 42-47.

Do istotnych zagrożeń zaliczane jest również złośliwe oprogramowanie infekujące sieci komputerowe oraz włamania do systemów płatności mobilnych[6]. Stanowi to wyzwanie nie tylko dla indywidualnych użytkowników, ale również dla kadry zarządzającej personelem przedsiębiorstw, który może być w szczególny sposób narażony na próby wyłudzenia poufnych informacji.

Celem pracy jest przedstawienie mechanizmu oszustwa internetowego typu „*spear phishing*" oraz ocena podatności pracowników jednego z podmiotów gospodarczych na próby wyłudzenia danych, umożliwiających przejęcie dostępu do służbowej skrzynki pocztowej. Celem pracy jest również analiza wiadomości e-mailowych, które odebrano na firmowej skrzynce pocztowej i sklasyfikowano jako próba wyłudzenia informacji lub infekcji złośliwym oprogramowaniem.

Za cel pracy obrano również opracowanie założeń niskonakładowego, uniwersalnego audytu wewnętrznego, który można przeprowadzić we wszystkich podmiotach, które udostępniają pracownikom konta służbowe chronione hasłem, bez względu na ich charakter. Audyt w sposób kontrolowany pozwoliłby na sondaż stopnia wyszkolenia i podatności pracowników na próby wyłudzenia poufnych danych. Na jego podstawie przełożeni mogliby ocenić zasadność przeprowadzenia doraźnych szkoleń pracowników w celu zminimalizowania zagrożeń wynikających z phishingu.

K. Materska[7] zwraca uwagę, że każdy zasób, który ma być źródłem przewagi konkurencyjnej dla organizacji, musi podlegać ochronie. Jednym z jej rodzajów jest prewencja w postaci szkoleń, stanowiących również podstawowe narzędzie rozwoju pracowników[8]. Są one rozumiane jako uczenie prostych umiejętności i nawyków, które są wykorzystywane w codziennej pracy.

2. Informacja jako zasób strategiczny

W klasycznej ekonomii zasoby rozumiane są jako czynniki produkcji, do których zalicza się zasoby materialne, w tym: rzeczowe, ludzkie oraz finansowe (ziemia, praca i kapitał)[9].

[6] Gordon S., Ford R.: On the definition and classification of cybercrime. „Journal in Computer Virology", No. 2(1), 2006, p. 13-20.

[7] Materska K.: Rozwój koncepcji informacji i wiedzy jako zasobu organizacji, [w]: Sosińska-Kalata B., Przastek-Samokowa M. (red.): Od informacji naukowej do technologii społeczeństwa informacyjnego. Miscellanea Informatologica Varsoviensia. SBP, Warszawa 2005, s. 199-216.

[8] Łazowski Sz.: Skuteczność szkoleń w małym przedsiębiorstwie, [w:] Zieliński M., Vogelgesang A. (red.): Gospodarowanie zasobami w przedsiębiorstwie – wybrane problemy. Przegląd nauk stosowanych 2, 2014, s. 44-52.

[9] Say J.B.: Traktat o ekonomii politycznej. PWN, Warszawa 1960.

Brózda i Marek[10] definiują zasoby jako czynniki wytwórcze znajdujące się w dyspozycji przedsiębiorstwa i wykorzystywane w procesie produkcji, podziału, wymiany i konsumpcji. Zasób to pewna ilość czegoś, co zostało zebrane i nagromadzone w celu wykorzystania w przyszłości. Jest to pewnego rodzaju rezerwa, zapas[11]. Zasoby materialne organizacji tworzy większość składników majątkowych odzwierciedlanych w bilansie.

Współcześnie do zasobów przedsiębiorstwa zalicza się również informację i wiedzę określane jako kapitał niematerialny, czy też aktywa wiedzy[12,13]. W epoce społeczeństwa informacyjnego nabrały one szczególnego znaczenia i stały się podstawowymi zasobami dynamicznie rozwijających się przedsiębiorstw[14]. Stanowią one potencjał strategiczny, są postrzegane jako główne źródło i siła napędowa wzrostu konkurencyjności. K. Materska[15] zwraca uwagę, że informacja i wiedza są zasobem strategicznym, jeśli stanowią o unikalności i przewadze konkurencyjnej firmy, a ich wartość wynika przede wszystkim z faktu ich wykorzystania. B. Czerniachowicz[16] zauważa, że zasoby informacji i wiedzy są urzeczywistniane przez ludzi w postaci kompetencji oraz urzeczywistniane przez samo przedsiębiorstwo, które posiada/wynajmuje lub tworzy te zasoby.

W XXI wieku informacja stanowi jeden z najważniejszych zasobów, którym może zarządzać organizacja[17]. Ma swój cykl życia obejmujący tworzenie, dystrybucję, wykorzystywanie i usuwanie, swoją wartość i wymaga poniesienia kosztów na jej pozyskanie. Może służyć realizacji określonych celów i podobnie jak inne zasoby może stać się obiektem kradzieży.

3. Zagrożenia informacji i infrastruktury teleinformatycznej

Informacje są nierozerwalnie związane z przechowywaniem, przetwarzaniem i udostępnianiem danych. Dane są pozyskiwane, gromadzone i poddawane analizom, często z wykorzystaniem nowoczesnych narzędzi komputerowych, w tym oprogramowania oraz

[10] Brózda J., Marek S.: Zasoby i ich znaczenie w działalności przedsiębiorstwa, [w:] Marek S., Białasiewicz M. (red.): Podstawy nauki o organizacji, PWE, Warszawa 2008.
[11] Stefanowicz B.: Informacja jako zasób strategiczny. „Ekonomika i Organizacja Przedsiębiorstwa", nr 7, 2004, s. 11-21.
[12] Best D.P.: Fourth Resource: Information and Its Management. Ashgate Publishing Company, Brookfield, VT, USA 1996.
[13] Murawska M.: Zarządzanie strategiczne niematerialnymi zasobami przedsiębiorstwa. Fundacja Promocji i Akredytacji Kierunków Ekonomicznych, Warszawa 2008.
[14] Kunasz M.: Zasoby przedsiębiorstwa w teorii ekonomii. „Gospodarka Narodowa", nr 10, 2006, s. 33-48.
[15] Materska K.: op.cit., s. 202.
[16] Czerniachowicz B.: Zasoby przedsiębiorstwa jako czynnik kreowania przewagi konkurencyjnej. Uniwersytet Szczeciński, Szczecin, 2012, s. 104.
[17] Barbachowska B.: Bezpieczeństwo informacji w firmie. „Journal of Modern Science", No. 2/13, 2012, p. 147-175.

cyfrowych nośników[18]. Jest to subtelna droga, jaką przechodzą dane, zanim zostaną przekształcone w informację. Żebrowski[19] przekonuje, że największym zagrożeniem dla zasobów danych i informacji stanowią błędy i pomyłki ludzkie, ale także działania celowe, polegające na umyślnym niszczeniu zasobów, zniekształcaniu i usuwaniu informacji, udostępnianiu haseł autoryzacji dostępu i inne.

Zdaniem Turskiego[20], komputery, informatyka i technologia informacyjna zrewolucjonizowały przemysł i sektor usług. Biegłość obsługi komputera oraz wybranych technik i narzędzi komputerowych jest obecnie wymagana nie tylko w coraz większej liczbie wykonywanych zawodów, ale również w życiu codziennym. Technologia informacyjna rozumiana jako posługiwanie się środkami i metodami informatyki w celu rozwiązania określonych problemów umożliwia człowiekowi aktywne funkcjonowanie w społeczeństwie informacyjnym.

Istnieje wiele różnorakich zagrożeń związanych z wykorzystaniem nowoczesnych technologii informacyjnych. Babik[21] dzieli je na: zagrożenia o charakterze psychologicznym (np. zatarcie granic pomiędzy rzeczywistością a światem wirtualnym), technicznym (zniszczenie sprzętu, utrata danych), medycznym (przypadłości wynikające z długotrwałej pracy z komputerem), prawnym (np. dotyczące praw autorskich) i społecznym (np. przemoc psychiczna w mediach społecznościowych). Stwierdza, że zagrożenia mogą mieć charakter globalny lub indywidualny, i mogą powodować uzależnienia.

Inny podział proponuje Bączek[22]. Dzieli on zagrożenia na losowe, rozumiane jako wszelkiego rodzaju klęski żywiołowe, katastrofy lub wypadki, które wpływają na nośniki informacji i infrastrukturę związaną z jej przechowywaniem; tradycyjne zagrożenia informacyjne, w tym szpiegostwo, działalność dywersyjna lub sabotażowa ukierunkowana na pozyskanie informacji lub dezinformację; zagrożenia technologiczne, związane z gromadzeniem, przechowywaniem, przetwarzaniem i przesyłem danych w sieciach teleinformatycznych oraz zagrożenia wynikające z niedostatecznych rozwiązań organizacyjnych i strukturalnych.

Żebrowski i Kwiatkowski[23] zagrożenia różnicują na wewnętrzne, zewnętrzne (powstające poza organizacją) i fizyczne. Zagrożenia wewnętrzne wiążą się z utratą danych przez

[18] Król K., Salata T.: Gromadzenie, przetwarzanie oraz wizualizacja danych przestrzennych za pomocą interaktywnych aplikacji internetowych na potrzeby rozwoju obszarów wiejskich. „Infrastruktura i Ekologia Terenów Wiejskich", nr 1/IV, 2013, s. 195-207.

[19] Żebrowski A.: Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa, [w:] Borowiecki R., Kwieciński M. (red.): Informacja i wiedza w zintegrowanym systemie zarządzania. Zakamycze, Kraków 2004, s. 421-446.

[20] Turski W.: Rola informatyki. Raport 3. Kongresu Informatyki Polskiej – Polska informatyka w Unii Europejskiej. Poznań-Warszawa 2003.

[21] Babik W.: op.cit., s. 5.

[22] Bączek P.: Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego. Adam Marszałek, Toruń 2006.

[23] Żebrowski A., Kwiatkowski M.: Bezpieczeństwo informacji III Rzeczypospolitej. Oficyna Wydawnicza Abrys, Kraków 2000.

uszkodzenie nośnika lub brakiem możliwości jego obsługi z powodu zdarzeń losowych, bądź też działań celowych. Zagrożenia zewnętrzne wiążą się z działaniami osób trzecich w stosunku do nośników danych bądź też użytkowników sieci, lub systemu. Fizyczne z kolei rozumieją jako zagrożenia związane z awarią, katastrofą lub innym zdarzeniem wpływającym na system informacyjny bądź infrastrukturę sieciową.

Klasyfikacji oraz charakterystyki zagrożeń występujących w Internecie podejmuje się również Król i Bedla[24]. Dzielą oni zagrożenia na mniej lub bardziej poważne w skutkach. Wyróżniają te, które mogą doprowadzić do utraty środków finansowych oraz inne, które bywają jedynie uciążliwe, np. wiadomości typu „*spam*". Szczególną uwagę przywiązują do zagrożeń, za którymi stoi bezpośrednio człowiek, takich jak: próby wyłudzania poufnych informacji osobistych, w tym kradzież tożsamości (ang. *phishing, pharming, spearphishing*), próby oszustw internetowych bazujące na ukrywaniu istotnych klauzur w obszernych regulaminach usług, lub oparte na informacjach pozyskanych z Internetu, wreszcie przemoc bezpośrednia (ang. *cyberbullying*) i pornografia.

Przedsiębiorstwa zwracają coraz więcej uwagi na zagrożenia związane z utratą bądź udostępnieniem informacji istotnych strategicznie. B. Barbachowska[25] zauważa, że problem bezpieczeństwa informacji nabrał szczególnego znaczenia w dobie dynamicznego rozwoju technologicznego, wraz z którym pojawiły się nowe zagrożenia bezpieczeństwa informacji. Zwraca szczególną uwagę na czynnik ludzki w analizie potencjalnych zagrożeń utraty danych. To użytkownicy nośników informacji oraz systemów komputerowych z autoryzowanym dostępem są w największym stopniu narażeni na zagrożenia związane z bezpieczeństwem informacji. Szczególnej roli nabierają tu systemy wczesnego ostrzegania i rozpoznania zagrożeń, które mogą być pomocne w identyfikacji symptomów świadczących o zagrożeniu informacji i pozwalają na podjęcie stosownych działań.

4. Charakterystyka phishingu

Phishing (ang. *password harvesting fishing*) jest rodzajem oszustwa internetowego, które wykorzystuje techniki psychologiczne[26]. W wolnym tłumaczeniu oznacza „*łowienie w sieci*" lub „łowienie siecią". Zwykle próba oszustwa ma charakter zautomatyzowany, masowy i globalny, a sprawcy są trudni do wykrycia. Ataki phishingowe służą przede wszystkim kradzieży środków finansowych poprzez próby wyłudzenia danych autoryzacji dostępu do:

[24] Król K., Bedla D.: Analiza wybranych zagrożeń związanych z promowaniem, sprzedażą i rezerwacją usług agroturystycznych w Internecie – studium przypadku. „Episteme", nr 22, t. 1, 2014, s. 5-13.

[25] Barbachowska B.: Bezpieczeństwo finansowe małych podmiotów gospodarczych, [w:] Lisiecki M., Raczkowska-Lipińska M. (red.): Zarządzanie bezpieczeństwem w Unii Europejskiej wobec globalnych zagrożeń. Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów 2008.

[26] Hong J.: The state of phishing attacks. „Communications of the ACM", No. 55(1), 2012, p. 74-81.

kont bankowych (numer klienta, kody jednorazowe dla przelewów, hasła), systemów płatności (np. *PayPal, American Express*), sklepów internetowych (z wykorzystaniem znanych marek np. *Amazon*), serwera poczty w celu rozsyłania wiadomości typu spam, podsłuchowi, szpiegostwu gospodarczemu, ale również mogą stanowić próbę zaszkodzenia indywidualnym użytkownikom. Zjawisko to nasila się, przyjmuje coraz bardziej wyszukaną i doskonalszą formę, również w postaci wiadomości SMS oraz VOIP (ang. *Voice Over Internet Protocol*), ponadto jest coraz częściej wykorzystywane przez amatorów na małą skalę.

Według badań Kaspersky Lab[27] w latach 2012-2013 ponad 37 milionów użytkowników na całym świecie zostało poddanych atakom phishingowym, co stanowi wzrost o 87% w stosunku do lat 2011-2012. Ataki phishingowe były najczęściej wymierzone w użytkowników Internetu w Rosji, Stanach Zjednoczonych, Indiach, Wietnamie oraz Wielkiej Brytanii. Celem ponad 20% wszystkich ataków były banki i inne organizacje finansowe lub kredytowe.

Atak phishingowy jest specyficzną formą cyberprzestępczości. W przeciwieństwie do szkodliwego oprogramowania tworzonego dla konkretnych systemów operacyjnych, phishing może być skuteczny na wszystkich urządzeniach z dostępem do Internetu. Atak phishingowy wykorzystuje zaufanie i znajomość marki lub skradzioną tożsamość. Polega na utworzeniu kopii, imitacji strony internetowej wybranej instytucji, której pracownik lub klient ma być zaatakowany. Atak stanowi próbę nakłonienia użytkownika do ujawnienia danych osobistych, zwykle za pośrednictwem formularza na tak spreparowanej stronie, w tym loginów, haseł, numerów PIN i wszelkich innych, które mogą być wykorzystane do uzyskania korzyści finansowych, kradzieży informacji, walki informacyjnej lub paraliżu informatycznego.

Szczególnym rodzajem phishingu jest phishing skierowany do konkretnej grupy odbiorców (ang. spear-phishing), zwany w żargonie „*phishingiem targetowanym*". W wolnym tłumaczeniu oznacza „*łowienie harpunem*". Stanowi on próbę wyłudzenia poufnych informacji za pomocą ukierunkowanej wiadomości e-mail. Oszust wykorzystuje informacje związane z potencjalną ofiarą pozyskane np. ze strony internetowej lub serwisów społecznościowych. Wiadomość jest przygotowana tak, aby sprawiała wrażenie wysłanej przez osobę, firmę lub instytucję znaną odbiorcy. Zwykle nadawca wiadomości podszywa się pod wybranego użytkownika Internetu, posługując się personaliami, a nawet fotografią pozyskaną w sieci.

[27] Kaspersky Lab: Ewolucja ataków phishingowych 2011-2013, http://goo.gl/bHfv3, dostęp: 15.05.2015.

5. Materiały i metody

Badanie podatności na atak phishingowy przeprowadzono w warunkach laboratoryjnych, w sposób kontrolowany, w ramach wewnętrznej infrastruktury sieciowej, dla podmiotu gospodarczego świadczącego usługi na rynku komercyjnym. Test przeprowadzono na wyselekcjonowanej grupie 26 pracowników wybranego działu firmy, z dbałością o formę najbardziej zbliżoną do tej, którą najczęściej przyjmują próby wyłudzenia poufnych danych związanych z autoryzacją dostępu do kont pocztowych. W badaniu zastosowano koncepcję z rodzaju „*ukryty klient*" (ang. *mystery shopping*)[28]. Służby informatyczne w sposób kontrolowany wystąpiły w roli oszusta podejmującego próbę wyłudzenia danych. Grupa testowanych użytkowników nie została poinformowana o udziale w badaniu w celu uwiarygodnienia jego wyniku.

Badanie sprowadzało się do obserwacji i odnotowania zachowań użytkowników służbowych skrzynek pocztowych w kontakcie ze specjalnie przygotowaną wiadomością e-mail. Z uwagi na fakt, że próby wyłudzenia poufnych danych są coraz bardziej wyszukane, treść rozesłanej wiadomości przyjęła formę spersonalizowaną, zgodnie ze specyfiką ataków typu „*spear phishing*"[29,30], z wykorzystaniem danych publicznie dostępnych na stronie internetowej badanego podmiotu. W treści zapytania znalazła się prośba o autoryzację dostępu do służbowego konta pocztowego z uwagi na wdrożenie nowej wersji systemu, zawierającą link do spreparowanego formularza. Wiadomość została podpisana imieniem i nazwiskiem fikcyjnego pracownika działu informatyki. Ponadto, czujność pracowników poddanych badaniu mogły uśpić częste zmiany wersji oprogramowania przeprowadzane w półroczu poprzedzającym wykonanie testu.

Formularz internetowy, którego zadaniem było przejęcie loginu i hasła do kont pocztowych, został spreparowany tak, aby do złudzenia przypominał ten, z którego korzystają pracownicy. Został jednak umieszczony na innym serwerze, w chronionej sieci wewnętrznej, która uniemożliwia dostęp osób postronnych.

Badania przeprowadzone przez R. Dhamija i współautorów[31] pokazują, że około 25% użytkowników witryn internetowych nie zwraca uwagi na newralgiczne punkty związane z bezpieczeństwem podczas jej przeglądania. Zaliczają do nich pasek adresu (domena, adres internetowy) oraz pasek stanu (ang. *status bar*). Może to mieć kluczowe znaczenie w obronie

[28] Hazlerig A.: Introduction to Mystery Shopping: The Perfect Home-based Business. Booksurge Publishing, North Charleston 2007.
[29] Parmar B.: Protecting against spear-phishing. „Computer Fraud & Security", No. 1, 2012, p. 8-11.
[30] Wang J., Herath T., Chen R., Vishwanath A., Rao H.R.: Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. „IEEE Transactions on Professional Communication", No. 55(4), 2012, p. 345-362.
[31] Dhamija R., Tygar J.D., Hearst M.: Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems. ACM New York, NY, USA 2006.

przed atakami typu phishing. Dlatego też spreparowany formularz poczty umieszczono pod innym adresem internetowym oraz z wykluczeniem szyfrowanej wersji protokołu HTTP (ang. *Hypertext Transfer Protocol Secure*) tak, aby otrzymana wiadomość mogła wzbudzić wątpliwości.

Analizę wiadomości e-mailowych spływających na firmowe skrzynki pocztowe umożliwiło utworzenie testowego adresu mailowego, który został opublikowany na stronie internetowej badanej firmy w formie odnośnika hipertekstowego, z pominięciem zabezpieczeń skryptowych. Tak opublikowany adres jest łatwo przechwytywany przez roboty spamowe i trafia do bazy adresatów niechcianych wiadomości.

Z uwagi na zastrzeżenia podmiotu, dla którego przeprowadzono badania, nazwa marki oraz zakres świadczonych usług pozostają znane jedynie autorowi badań.

6. Wyniki i wnioski

Monitoring wiadomości e-mailowych prowadzono 10 miesięcy, w okresie od 1 sierpnia 2014 roku do 31 maja 2015 roku (304 dni). W okresie tym zebrano ogółem 5963 wiadomości typu spam (tab. 1), co daje średnio około 20 niechcianych wiadomości dziennie, tylko z jednego adresu mailowego. Znakomita większość to wiadomości śmieci związane z reklamą najróżniejszych towarów i usług. W gronie odebranych wiadomości zidentyfikowano 49 niebezpiecznych, stanowiących próbę wyłudzenia danych, pieniędzy lub infekcji komputera złośliwym oprogramowaniem. Niepokojącym zjawiskiem są e-maile (5 przypadków), których załącznik stanowi koń trojański w formie skompresowanego pliku, przedstawiony jako wezwanie do zapłaty zaległej faktury. W przedsiębiorstwach, które dokonują licznych operacji finansowych, ryzyko otwarcia tak spreparowanej wiadomości jest duże. Innym fortelem stosowanym przez oszustów była informacja o dokonanej rezerwacji podróży z wezwaniem do jej potwierdzenia lub odrzucenia, powodująca infekcję złośliwym oprogramowaniem (2 przypadki).

Większość wiadomości stanowiły próby wyłudzenia loginu i hasła do skrzynki pocztowej (37 przypadków). Przyjmowały one postać ostrzeżeń o wykorzystaniu limitu przestrzeni serwera dla konta pocztowego, prośby o weryfikację danych autoryzacji połączenia, wezwania do weryfikacji tożsamości poprzez zalogowanie się, lub ostrzeżenia o zablokowaniu konta. Kolejne trzy wiadomości stanowiły próbę wyłudzenia loginu i hasła do bankowości elektronicznej PKO Bank Polski oraz iPKO Bank.

Dwie wiadomości przyjęły formę groźby pozwu sądowego w kontekście rzekomych nieprawidłowości w regulaminach zamieszczonych na stronie internetowej firmy.

Po weryfikacji treści oraz podmiotu, który je przysłał, stwierdzono, że są to próby wyłudzenia środków finansowych.

Tabela 1

Rodzaj oraz liczba zidentyfikowanych zagrożeń

Charakter wiadomości e-mail	Liczba wiadomości
Wiadomość typu spam	5963
Potencjalnie niebezpieczna wiadomość	49
Próby wyłudzenia danych autoryzacji dostępu do konta pocztowego	37
Próby wyłudzenia danych autoryzacji dostępu do konta bankowego	3
Próby wyłudzenia środków finansowych	4
Próby zainfekowania komputera koniem trojańskim	5

Źródło: Badania własne.

Liczba regularnie ponawianych ataków oraz stopień zagrożenia utratą danych oraz przejęcia dostępu do służbowej poczty potwierdziły zasadność przeprowadzenia audytu.

Pomimo iż w opinii kadry zarządzającej liczba oraz forma wewnętrznych kampanii informacyjnych na temat zagrożeń związanych z wyłudzeniem poufnych danych jest wystarczająca, spośród 26 osób poddanych badaniu, login i hasło dostępu do służbowej skrzynki pocztowej ujawniło 5 pracowników. Ujawnienie danych autoryzacji dostępu w warunkach rzeczywistych mogłoby mieć znaczące skutki dla bezpieczeństwa wewnętrznej sieci komputerowej, w tym dla oprogramowania obsługującego klienta poczty.

Grono osób poddanych badaniu zostało zaproszone na spotkanie szkoleniowe, gdzie przedstawiona została koncepcja testu oraz jego wyniki. W stosunku do pracowników, którzy udostępnili poufne dane nie zostały wyciągnięte konsekwencje służbowe. Ich tożsamość pozostaje znana jedynie przełożonym wyższego szczebla. Zostali oni wezwani na indywidualną rozmowę szkoleniową.

Analiza zebranych wiadomości mailowych oraz test przeprowadzony na wyselekcjonowanej grupie użytkowników wykazały, że w świetle skali działalności podmiotu oraz liczby zatrudnionych pracowników mających dostęp do infrastruktury i strategicznych danych służbowych istnieje potrzeba przeprowadzania regularnych szkoleń i audytów wewnętrznych bezpieczeństwa. Stąd też przyjęto strategię, że każdy zatrudniony pracownik przechodząc szkolenie z zakresu bezpieczeństwa i higieny pracy zostanie również przeszkolony z zakresu zagrożeń związanych z udostępnieniem poufnych danych oraz konsekwencji, jakie może z tego tytułu ponieść on sam oraz firma.

W przeprowadzonych badaniach ujawniły się trzy zasadnicze postawy użytkowników wobec próby ataku phishingowego. Za kryterium podziału obrano sposób postępowania w kontakcie z potencjalnie niebezpieczną wiadomością. Pierwsza postawa charakteryzuje użytkowników biernych. Jest to najliczniejsza grupa. Zwykle rozpoznają oni zagrożenie i nie podejmują żadnych czynności związanych z wiadomością e-mail, która wzbudziła ich wątpliwość. Druga to postawa aktywna. Osoby te charakteryzują się pewną dynamiką

działania. Podejmują czynności służące weryfikacji treści otrzymanej wiadomości. Rozpytują w odpowiednich komórkach firmy w celu potwierdzenia jej wiarygodności. W gronie badanych osób znalazły się dwie, które kontaktowały się z działem informatyki w celu weryfikacji tożsamości pracownika, którego nazwiskiem podpisano wątpliwą wiadomość.

Do ostatniej grupy zaliczyć można użytkowników, którzy udzielili odpowiedzi na otrzymaną wiadomość, udostępniając dane związane z autoryzacją dostępu do kont chronionych. Relatywnie nieduża próba badawcza nie pozwala wypracować ogólnego rysu psychologicznego, czy też zestawu cech osobowych użytkowników, którzy są mniej lub bardziej podatni na ataki phishingowe.

7. Podsumowanie

Całkowite bezpieczeństwo danych i informacji strategicznych dla przedsiębiorstwa jest trudne, lub wręcz niemożliwe do osiągnięcia. Skuteczność, zakres oraz skala działań mających na celu minimalizowanie zagrożeń bezpieczeństwa informacji i systemów teleinformatycznych w dużej mierze zależy od kadry zarządzającej. Spoczywa na niej zadanie identyfikacji zagrożeń, sformułowania oraz realizacji polityki bezpieczeństwa informacji, jednak w ścisłej współpracy z działem informatyki, który odpowiada za techniczne aspekty audytu.

Nie wszystkie podejmowane działania muszą wiązać się z poniesieniem wysokich kosztów. W wybranych przypadkach realizacja audytu wewnętrznego oparta na własnej kadrze i infrastrukturze może przyczynić się do poprawy bezpieczeństwa informacji.

W praktyce okazuje się, że najsłabszym ogniwem łańcucha bezpieczeństwa informacji i systemów teleinformatycznych jest człowiek. Działania podjęte w badanym podmiocie posłużyły jako podstawa dla koncepcji wewnętrznego audytu bezpieczeństwa danych w zakresie możliwości udostępnienia ich przez pracowników osobom postronnym. Przedstawiona w pracy koncepcja stanowi propozycję identyfikacji oraz ograniczenia istniejących zagrożeń zewnętrznych. Ma ona swoje wady i zalety. Wprowadza wśród pracowników swoisty stan gotowości. Podnosi czujność i nieufność do wiadomości mailowych budzących wątpliwość. Może stanowić materiał wyjściowy dla szkoleń i kampanii informacyjnych w zakresie bezpieczeństwa i ochrony danych. Jest niskonakładowa, realizowana za pomocą wewnętrznej infrastruktury i oprogramowania. Pozostaje w pełnej kontroli wewnętrznych służb informatycznych. Dostarcza kadrze zarządzającej informacji na temat rzeczywistego stopnia przeszkolenia i świadomości pracowników na temat zagrożeń związanych z udostępnianiem poufnych danych.

Koncepcja audyt może budzić kontrowersje wśród samych pracowników, którzy mogą odnieść wrażenie, że są obserwowani i oceniani. Ponadto osoby, które padły ofiarą ataku, mogą poczuć się gorsze lub winne. Kwestie te powinny być dokładnie omówione przez przełożonych podczas indywidualnych rozmów szkoleniowych.

Z założenia audyt nie przewiduje konsekwencji służbowych wobec osób, które udostępniły dane. Istnieje jednak niebezpieczeństwo napiętnowania (wypominanie, podświadoma niechęć, wywieranie presji, szykany) takich osób przez kadrę zarządzającą. Dlatego też możliwe jest przeprowadzenie audytu z całkowitym ukryciem tożsamości osób biorących udział w badaniu i ograniczeniu spotkań do grupowych szkoleń.

W opisie badań celowo pominięto kwestie techniczne związane z przygotowaniem formularza, wykorzystanymi narzędziami oraz sposobem przejęcia i odczytu haseł tak, aby nie tworzyć instruktarzu dla osób działających w złej wierze.

Serwery sieciowe nie znają ograniczeń wizowych. Rosnąca liczba udostępnianych nieodpłatnie narzędzi informatycznych typu OpenSource oraz dostęp do ogólnoświatowej infrastruktury sieciowej, w tym serwerów oraz poczty internetowej, sprawia, że próby wyłudzeń poufnych danych stanowią realne zagrożenia dla bezpieczeństwa informacji. W działaniach przeciwko użytkownikom usług wymagających autoryzacji dostępu wykorzystywana jest znajomość psychologii i zachowań społecznych.

Liczne podmioty gospodarcze, głównie w celach marketingowych, wychodząc naprzeciw klientom lub użytkownikom, udostępniają wiele informacji, które mogą zostać wykorzystane przeciwko nim. Dlatego też nieodzowne są działania edukacyjne prowadzone w każdym podmiocie, który ma świadomość, że jego pracownicy operują na danych mogących mieć kluczowe znaczenie. Mowa tu przede wszystkim o danych strategicznych gospodarczo oraz danych osobowych.

Problem wyłudzania poufnych danych najsilniej odczuwany jest przez podmioty świadczące usługi komercyjne, przede wszystkim finansowe oraz strategiczne jednostki rządowe. W ostatnich latach nabiera także szczególnego znaczenia w jednostkach szkolnictwa każdego szczebla. Rośnie również liczba amatorskich prób wyłudzenia danych przeprowadzana na gruncie towarzyskim w celu czynienia szkody emocjonalnej, noszącej znamiona przemocy.

Popularność ataków phishingowych rośnie również z uwagi na relatywnie prosty mechanizm ich przeprowadzenia oraz dużą skuteczność. Niebagatelną rolę odgrywa tu rozmiar grupy docelowej oraz automatyzacja procesu pozyskiwania adresów mailowych z sieci i rozsyłania wiadomości. Przestępcy bez skrupułów wykorzystują także zaufanie do znanych marek oraz naiwność, przyzwyczajenia i niewiedzę użytkowników sieci.

Znajomość taktyk phishingowych oraz opracowanie procedur postępowania w przypadku wiadomości budzących wątpliwość może zmniejszyć ryzyko utraty danych. Pracownicy,

którzy zostali przeszkoleni w zakresie bezpieczeństwa informacji i systemów teleinformatycznych, będą rozważniej korzystali z zasobów własnych i firmowych.

Bibliografia

1. Babik W.: Ekologia informacji – wyzwanie XXI wieku. „Praktyka i Teoria Informacji Naukowej i Technicznej", nr (1)37, 2002.
2. Barbachowska B.: Bezpieczeństwo finansowe małych podmiotów gospodarczych, [w:] Lisiecki M., Raczkowska-Lipińska M. (red.): Zarządzanie bezpieczeństwem w Unii Europejskiej wobec globalnych zagrożeń. Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów 2008.
3. Barbachowska B.: Bezpieczeństwo informacji w firmie. „Journal of Modern Science", No. 2/13, 2012.
4. Bączek P.: Zagrożenia informacyjne a bezpieczeństwo państwa Polskiego. Adam Marszałek, Toruń 2006.
5. Best D.P.: Fourth Resource: Information and Its Management. Ashgate Publishing Company, Brookfield, VT, USA 1996.
6. Brózda J., Marek S.: Zasoby i ich znaczenie w działalności przedsiębiorstwa, [w:] Marek S., Białasiewicz M. (red.): Podstawy nauki o organizacji. PWE, Warszawa 2008.
7. Castells M.: The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I. Malden, MA; Oxford, UK: Blackwell 2009.
8. CBOS: Internauci 2014. Centrum Badania Opinii Społecznej, Warszawa 2014.
9. Czerniachowicz B.: Zasoby przedsiębiorstwa jako czynnik kreowania przewagi konkurencyjnej. Uniwersytet Szczeciński, Szczecin 2012.
10. Dhamija R., Tygar J.D., Hearst M.: Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems. ACM New York, NY, USA 2006.
11. Gordon S., Ford R.: On the definition and classification of cybercrime. „Journal in Computer Virology", No. 2(1), 2006.
12. Hazlerig A.: Introduction to Mystery Shopping: The Perfect Home-based Business. Booksurge Publishing, North Charleston 2007.
13. Hong J.: The state of phishing attacks. „Communications of the ACM", No. 55(1), 2012.
14. Kaspersky Lab: Ewolucja ataków phishingowych 2011-2013, http://goo.gl/bHfv3, dostęp: 15.05.2015.
15. Król K., Bedla D.: Analiza wybranych zagrożeń związanych z promowaniem, sprzedażą i rezerwacją usług agroturystycznych w Internecie – studium przypadku. Episteme, nr 22, t. 1, 2014.

16. Król K., Salata T.: Gromadzenie, przetwarzanie oraz wizualizacja danych przestrzennych za pomocą interaktywnych aplikacji internetowych na potrzeby rozwoju obszarów wiejskich. „Infrastruktura i Ekologia Terenów Wiejskich", nr 1/IV, 2013.
17. Kunasz M.: Zasoby przedsiębiorstwa w teorii ekonomii. „Gospodarka Narodowa", nr 10, 2006.
18. Łazowski Sz.: Skuteczność szkoleń w małym przedsiębiorstwie, [w:] Zieliński M., Vogelgesang A. (red.): Gospodarowanie zasobami w przedsiębiorstwie – wybrane problemy. Przegląd nauk stosowanych 2, 2014.
19. Materska K.: Rozwój koncepcji informacji i wiedzy jako zasobu organizacji, [w]: Sosińska-Kalata B., Przastek-Samokowa M. (red.): Od informacji naukowej do technologii społeczeństwa informacyjnego. Miscellanea Informatologica Varsoviensia. SBP, Warszawa 2005.
20. Murawska M.: Zarządzanie strategiczne niematerialnymi zasobami przedsiębiorstwa. Fundacja Promocji i Akredytacji Kierunków Ekonomicznych, Warszawa 2008.
21. Parmar B.: Protecting against spear-phishing. „Computer Fraud & Security", No. 1, 2012.
22. Provos N., Rajab M. A., Mavrommatis P.: Cybercrime 2.0: when the cloud turns dark. „Communications of the ACM", No. 52(4), 2009.
23. Say J.B.: Traktat o ekonomii politycznej. PWN, Warszawa 1960.
24. Stefanowicz B.: Informacja jako zasób strategiczny. „Ekonomika i Organizacja Przedsiębiorstwa", nr 7, 2004.
25. Turski W.: Rola informatyki. Raport 3. Kongresu Informatyki Polskiej – Polska informatyka w Unii Europejskiej. Poznań-Warszawa 2003.
26. Wall D.S.: Cybercrime: The Transformation of Crime in the Information Age. Polity Press, Cambridge, UK 2007.
27. Wang J., Herath T., Chen R., Vishwanath A., Rao H.R.: Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. „IEEE Transactions on Professional Communication", No. 55(4), 2012.
28. Żebrowski A., Kwiatkowski M.: Bezpieczeństwo informacji III Rzeczypospolitej. Oficyna Wydawnicza Abrys, Kraków 2000.
29. Żebrowski A.: Bezpieczeństwo wiedzy – nowy atrybut działalności przedsiębiorstwa, [w:] Borowiecki R., Kwieciński M. (red.): Informacja i wiedza w zintegrowanym systemie zarządzania. Zakamycze, Kraków 2004.