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

ORGANIZACYJNE ASPEKTY WALKI ZE SPAMEM Z PUNKTU WIDZENIA PRZECIĘTNEGO UŻYTKOWNIKA

Streszczenie. W artykule poruszono kwestie niechcianych wiadomości elektronicznych, które zalewają w ostatnich latach skrzynki pocztowe użytkowników z całego świata. W pracy przedstawiono relację z eksperymentu przeprowadzonego w jednej z firm. Polegał on na monitorowaniu wiadomości typu spam odbieranych przez skrzynki pocztowe pracowników. Badania pozwoliły zidentyfikować newralgiczne kwestie związane z udostępnianiem służbowych adresów mailowych. Na podstawie poczynionych obserwacji przygotowano cykl szkoleń, których celem było zminimalizowanie zjawiska spamu.

Słowa kluczowe: ochrona przed spamem, niechciane e-maile, zagrożenia w Internecie

ORGANIZATIONAL ASPECTS OF THE FIGHT AGAINST SPAM FROM THE POINT OF VIEW OF AN AVERAGE USER

Abstract. The article discusses the issues of unwanted electronic messages that in recent years are flooding mailboxes of users from all around the world. The paper presents an account of an experiment conducted in one of the companies. The experiment consisted of the monitoring of spam messages received on mailboxes of employees. The study has identified critical issues related to the security of corporate e-mail addresses. On the basis of these findings we prepared a series of trainings aimed at minimizing the phenomenon of spam.

Keywords: spam protection, unsolicited junk e-mail, Internet threats

1. Wstęp

Rozwój technik i narzędzi komputerowych, w szczególności programistycznych powoduje pojawianie się nowych funkcjonalności, dzięki którym witryny internetowe pełnią coraz to nowe funkcje. Internet zyskuje na znaczeniu jako płaszczyzna komunikacji, staje się wirtualną przestrzenią interakcji. Coraz szersze spektrum codziennych aktywności przenoszonych jest do sieci, a jej dynamiczny rozwój powoduje pojawianie się całkiem nowych, dotychczas niespotykanych[1].

Internet to nie tylko infrastruktura techniczna, to również dane i informacje oraz ludzie, którzy je tworzą. Internet stanowi sieć globalną, z której w 2014 roku korzystało już niemal 3 miliardy użytkowników, co stanowiło blisko 40% populacji[2,3]. Globalna sieć usprawnia komunikację, jej wykorzystanie niweluje barierę przestrzenną i czasową. Charakteryzuje ją dostępność, interaktywność oraz elastyczne formy przekazu[4].

Internet wpłynął na sposób prowadzenia działalności gospodarczej i stworzył nowe możliwości w zakresie promocji i sprzedaży produktów i usług. Jednak w cieniu jego licznych zalet pozostają często zagrożenia, jakie mogą się wiązać z jego wykorzystaniem, oraz zjawiska, które bywają uciążliwe dla użytkowników. Jednym z najbardziej powszechnych jest spam, który przyjmuje coraz to bardziej wyszukane formy i często stanowi narzędzie w rękach oszustów.

Bezpieczeństwo jest jedną z podstawowych potrzeb człowieka. Zapewnienie bezpieczeństwa coraz większej liczbie czynności wykonywanych w sieci oraz korzystania z rosnącej liczby różnorakich aplikacji sieciowych stanowi wyzwanie zarówno na gruncie technicznym, jak i edukacyjnym[5]. Zagrożenia występujące w wirtualnej przestrzeni są powodowane przez użytkowników z realnego świata i mogą mieć bezpośrednie i wymierne przełożenie na konsekwencje w życiu codziennym[6].

Celem pracy jest analiza struktury wiadomości typu spam odbieranych przez elektroniczną skrzynkę pocztową oraz odnotowanie zagrożeń, które w nich występują, z punktu widzenia przeciętnego użytkownika. W badaniach podjęto próbę identyfikacji form,

[1] Miller P.: Wprowadzenie do obserwacji online: warianty i ograniczenia techniki badawczej. „Przegląd Socjologii Jakościowej", nr 1, 2012, s. 76-97.
[2] ITU, The World in 2014: ICT Facts and Figures, International Telecommunication Union (ITU 2015), http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf, 10.12.2015.
[3] Kos-Łabędowicz J., Talar S.: Rola internetu w procesie zmian międzynarodowych stosunków gospodarczych. „Studia Ekonomiczne", nr 218, 2015, s. 75-87.
[4] Chełstowski D., Szewczyk A.: Problemy rozwoju handlu elektronicznego w Polsce. Zeszyty Naukowe. Studia Informatica, nr 30. Uniwersytet Szczeciński, Szczecin 2012, s. 21-44.
[5] Gostomski E., Michałowski T.: Rola Internetu w handlu międzynarodowym. „Współczesna Gospodarka", nr 5(3), 2014, s. 11-25.
[6] Bukowska E., Filipowska A., Abramowicz W.: Zapewnienie bezpieczeństwa przez semantyczne monitorowanie cyberprzestrzeni. „E-mentor", nr 3 (50), 2013, s. 11-17.

jakie przyjmują próby wyłudzenia poufnych danych oraz próby zainfekowania komputera złośliwym oprogramowaniem.

2. Pojęcie spamu i istota spammingu

Słowo „*spam*" pochodzi z języka angielskiego i stanowi skrót od *spiced pork and ham*, co oznacza mielonkę, i oddaje charakter wiadomości uznawanych za spam[7,8]. Pojęciem spamu określane są „wiadomości śmieci", niechciana korespondencja lub niepotrzebne wiadomości elektroniczne (ang. *junk-mail*), nazywane również „elektroniczną makulaturą". Maik[9] opisuje spam również jako cyt. *nadmiar informacji, które są zbędne dla odbiorcy przekazu*. Ponadto wiadomości przesłane drogą elektroniczną są kwalifikowane jako spam, gdy spełniają kilka określonych warunków:

1. Treść wiadomości jest niezależna od tożsamości odbiorcy.
2. Wiadomości przyjmują charakter komercyjny (oferta handlowa, reklama, ang. *Unsolicited Commercial Email*, UCE) i nie były w żaden sposób zamówione przez odbiorcę, przy czym cyt. *Informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny*[10]. W wybranych przypadkach wiadomości mogą zawierać treści polityczne, ideologiczne lub charytatywne, przyjmują wtedy formę informacji rozsyłanych w kampaniach społecznych, mniejszych lub większych kampaniach informacyjnych, prowadzonych również przez osoby prywatne (ang. *Unsolicited Bulk Email*, UBE).
3. Zamierzeniem nadawcy jest osiągnięcie określonych korzyści, zwykle majątkowych.

Konwencjonalna forma spamu ewoluuje. Spam to już nie tylko wiadomości śmieci otrzymywane drogę elektroniczną. Spamem określane są również niezamówione i niechciane treści rozprowadzane w komunikatorach internetowych, w sieciach społecznościowych oraz na forach i blogach tematycznych. Często treści te przedstawiają nieprawdziwy, fałszywy opis rzeczywistości, zwykle ukierunkowany na określony cel. Może on być polityczny – propagandowy bądź też czysto komercyjny[11]. Rozsyłanie spamu określane jest mianem

[7] Waglowski P.: Spam w formie niezamówionej informacji handlowej jako delikt nieuczciwej konkurencji, [w:] Tubielewicz A. (red.): Problemy informatyki w zarządzaniu. Politechnika Gdańska, Gdańsk 2003, s. 83-108.
[8] Czyżak M.: Spamming i jego karalność w polskim systemie prawnym. Pomiary, Automatyka, Kontrola, nr 55, 2009, s. 548-551.
[9] Maik A.: Ochrona przed spamem w przepisach. „Folia Bibliologica", nr 57, 2015, s. 81.
[10] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 Nr 144, poz. 1204, art. 10.
[11] Crawford M., Khoshgoftaar T.M., Prusa J.D., Richter A.N., Al Najada H.: Survey of review spam detection using machine learning techniques. "Journal of Big Data". Vol. 2(1), 2015, p. 1-24.

spamowania (ang. *spamming*), a jednostki zaangażowane w ten proceder są nazywane „spamerami" (ang. *spammer*).

Spamming jest formą przestępczości internetowej (cyberprzestępczości), stanowi działanie zabronione prawem, dokonywane zwykle przy pomocy komputera za pośrednictwem Internetu. Istotą spamowania jest rozsyłanie dużej liczby wiadomości o jednakowej treści do szerokiego grona odbiorców. Zjawisko to ma obecnie charakter powszechny i masowy. Ustawodawstwo polskie[12] określa spamming jako cyt. *przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy, będącego osobą fizyczną, za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej*.

Spam stanowi narzędzie, które jest powszechnie wykorzystywane do działań na szkodę użytkowników usług sieciowych. Coraz częściej spam wykorzystywany jest jako narzędzie mniej lub bardziej wyrafinowanych oszustw. W raporcie „*2015 Internet Security Threat Report*" wydawanym przez firmę Symantec[13], rok 2014 scharakteryzowano jako rok – luk bezpieczeństwa w oprogramowaniu, szybszych i doskonalszych ataków phishingowych oraz licznych przypadków blokowania plików użytkowników celem uzyskania okupu (ang. *ransomware*). Ponadto w 2014 roku odnotowano więcej komputerów zainfekowanych złośliwym oprogramowaniem niż w latach poprzednich. W raporcie zwrócono uwagę na wzrost liczby ataków ukierunkowanych na małe i średnie przedsiębiorstwa, które lokowane są w grupie szczególnego ryzyka. Podmioty te często nie przywiązują należytej wagi lub wręcz lekceważą kwestie zarządzania bezpieczeństwem danych. Wynika to przede wszystkim z niewiedzy i braku środków finansowych. Ponadto, raport zwraca szczególną uwagę na ataki typu spear phishing. Wiadomości mailowe, które przyjmują postać zbliżoną lub identyczną jak poczta firmowa, bądź też naśladują wiadomości od zaufanego partnera biznesowego, są wymieniane jako jeden z wysoko skutecznych sposobów infiltracji komputerów firmowych. Wszystko to stawia spam w innym świetle i sprawia, że nie może on być postrzegany jedynie jako wiadomości śmieci.

3. Spam i zagrożenia w bankowości elektronicznej

W dobie powszechnego dostępu do Internetu coraz więcej spraw załatwić można za pośrednictwem urządzeń z dostępem do sieci, bez wychodzenia z domu. Z punktu widzenia użytkownika do największych udogodnień wynikających z wykorzystania usług sieciowych zaliczyć można m.in. zakupy i rezerwacje w sklepach internetowych, możliwość poznawania

[12] Ustawa z dnia 18 lipca 2002 r., op. cit., art. 10.

[13] Symantec, The 2015 Internet Security Threat Report from Symantec, Vol. 20, April 2015, http://www.symantec.com/security_response/publications/threatreport.jsp, 01.12.2015.

opinii na temat produktów i ofert oraz ich porównywania, dogodne formy płatności oraz brak kolejek. Często jednak ułatwieniom tym towarzyszą zagrożenia, które przyjmują postać ataków wymierzonych w użytkowników kont internetowych – pocztowych, bankowych i innych. Aplikacje sieciowe i infrastruktura banków, a także portali udostępniających usługi sieciowe są zwykle lepiej zabezpieczone niż urządzenia klientów, dlatego też oszuści skupiają się na użytkownikach końcowych, działając tak, aby wykorzystać ich nieuwagę lub niewiedzę, często z zastosowaniem różnorakich socjotechnik[14].

Wiele zmian zachodzących w sektorze usług bankowych w dużej mierze wynika z rozwoju technologicznego. Znakomita większość transakcji finansowych odbywa się za pośrednictwem Internetu, gdzie pieniądz przyjmuje formę niematerialną i staje się informacją[15]. Wiąże się z tym wiele udogodnień, ale również zagrożeń. Najczęściej zgłaszaną przez użytkowników bankowości internetowej próbą oszustwa jest phishing (i jego różne odmiany) oraz szkodliwe oprogramowania typu *koń trojański*. Oszuści posuwają się również do preparowania fałszywych witryn internetowych, których zadaniem jest imitowanie tych prawdziwych[16]. Próby wyłudzenia informacji przyjmują coraz bardziej wyrafinowane formy. Klienci banków są namawiani przez oszustów do podania loginu i hasła chroniącego dostęp do konta bankowego, kodów jednorazowych umożliwiających wykonanie transakcji finansowych, instalacji dodatkowego oprogramowania, które rzekomo ma umożliwić lub usprawnić logowanie w serwisie bankowości elektronicznej. Wszystko to coraz częściej, również drogą telefoniczną – vishing (ang. *voice phishing*), stanowi próbę bezpośredniego, telefonicznego wyłudzenia danych autoryzacji dostępu do kont bankowych.

Instytucje finansowe odnotowują wzrost liczby fałszywych maili, które zawierają pliki ze złośliwym oprogramowaniem. W mailach tych oszuści często podszywają się pod znane firmy lub marki (w Polsce są to najczęściej: DHL, UPC, Poczta Polska, Netia, Orange, Play, inPost, Pekao, PKO Bank Polski i inne) i namawiają do wykonania określonej czynności, np. pobrania i wydruku faktury, ogłoszenia, rzekomo zawartej umowy lub też odesłania danych osobowych, co ma być konieczne do wypłaty rzekomej nagrody. W rzeczywistości zadaniem wiadomości jest zainfekowanie komputera złośliwym oprogramowaniem, co w przypadku bankowości elektronicznej służy przejęciu środków finansowych użytkownika.

M. Czyżak[17] zwraca uwagę, że dostępność oraz rozwój usług świadczonych za pośrednictwem Internetu zależy w dużej mierze od wiarygodności, bezpieczeństwa

[14] Pekao, Najważniejsze zasady, których warto przestrzegać, płacąc online. Biuletyn Bezpieczny Internet. Luty 2015, https://www.pekao24.pl/MCP/client/logon/bi_pdf/SafeInternet022015.pdf, 03.12.2015.
[15] Brzostowski T.: Innowacje, technologie, zagrożenia w świecie XXI wieku – z perspektywy finansów. Alterum, Warszawa 2012, s. 4.
[16] Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F.: Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia. KNF, Warszawa 2010, s. 29.
[17] Czyżak M.: op.cit., s. 48.

i niezawodności technologii teleinformatycznych. W przypadku bankowości elektronicznej będzie to bezpieczeństwo środków na rachunkach bankowych oraz bezpieczeństwo realizowanych transakcji. Coraz większa liczba wiadomości śmieci, wirusów, programów szpiegujących (ang. *spyware*) oraz innych form szkodliwego oprogramowania (ang. *malware*) przyczynia się do spadku zaufania użytkowników do usług sieciowych. Dalszy ich rozwój jest więc zależny od bezpieczeństwa ich realizacji. Zależy również od wiedzy i świadomości użytkowników, gdyż nawet najbardziej zaawansowane oprogramowanie komputerowe nie zapobiegnie kradzieży środków finansowych, w momencie gdy dane autoryzacji dostępu zostaną ujawnione bezpośrednio przez samego użytkownika[18].

4. Materiały i metody

W raportach na temat spamu podawane są zwykle dane o globalnym charakterze, które pokazują światową skalę i natężenie tego zjawiska, często w ujęciu procentowym[19]. Często w interpretacji tak przedstawionych danych brak jest punktu odniesienia względem jednostki. Pojawia się więc pytanie, ile spamu otrzymuje przeciętny użytkownik skrzynki pocztowej w zadanym okresie czasu? Jaka jest struktura tych maili, czego one dotyczą? Jak często stanowią próbę oszustwa? Wreszcie, jak wiele przestrzeni dysku serwera zajmuje spam tylko jednego, przeciętnego użytkownika?

W niniejszej pracy podjęto próbę zbadania, jaką strukturę ma spam odbierany przez przeciętnego użytkownika poczty elektronicznej jednej z firm, w której przeprowadzono badania. Szczególną uwagę poświęcono rozmiarom odbieranego spamu. Pomiary miały odpowiedzieć na pytanie, ile miejsca na dyskach twardych firmowych serwerów zajmować może spam tylko u jednego użytkownika, i jak się to przekłada na całą firmę?

W eksperymencie wykorzystano dwa adresy mailowe: służbowy (firmowy) oraz prywatny, założony w domenie jednego z czołowych portali informacyjnych w Polsce. Obydwa adresy umieszczono w publicznych i eksponowanych miejscach w sieci – adres służbowy na witrynach firmowych (zgodnie z rutynową praktyką firmy), adres prywatny wykorzystywano do rejestracji w portalach internetowych, forach i kontach społecznościowych. Wiadomości mailowe typu spam zbierane były od 3 sierpnia 2014 roku do 30 listopada 2015 roku (17 miesięcy).

[18] Król K.: Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu. Organizacja i Zarządzanie, nr 2(30), 2015, s. 19-32.

[19] Security Response, Symantec Security Response – malware, security risks, vulnerabilities, and spam, http://www.symantec.com/security_response/landing/spam, 01.12.2015.

Ponieważ w firmie, w której prowadzono monitoring poczty, często zgłaszane były próby ataków phishingowych, które kilkakrotnie zakończyły się powodzeniem (pracownicy zdradzali hasła dostępu), postanowiono zbadać strukturę maili phishingowych oraz odnotować ich liczbę. Wszystko to miało posłużyć do przygotowania szkoleń dla kadry, z zakresu bezpieczeństwa danych z przedstawieniem wyników monitoringu oraz realnie odnotowanych w firmie przypadków. Swoistym punktem odniesienia dla konta służbowego były badania prowadzone równolegle z wykorzystaniem konta prywatnego. Miały one służyć przede wszystkim lepszemu naświetleniu problemu spamu i ochrony przed spamem pracowników firmy.

Identyfikację treści oraz formy, jaką przyjmowały badane wiadomości, wykonano opierając się na wybranych aspektach metodyki opracowanej przez Symantec[20], jednego z największych w świecie producentów oprogramowania wspierającego bezpieczeństwo danych i zarządzanie informacjami. Posłużono się również metodą „identyfikacji maili po słowach kluczowych", która polega na klasyfikowaniu spamu według przyjętej hierarchii. Ze względu na zastrzeżenia firmy, w której przeprowadzono badania oraz fakt, że stanowią one fragment złożonego audytu bezpieczeństwa danych, domena, w której założono konto służbowe, pozostaje do wiadomości autora badań.

5. Wyniki badań i wnioski

Podczas trwania eksperymentu łącznie zebrano 6046 wiadomości w ramach skrzynki pocztowej prywatnej oraz 9903 w ramach skrzynki służbowej. Na firmowej skrzynce pocztowej znacznie częściej odbierano wiadomości związane z ofertą różnorakich szkoleń, konferencji i kursów, często o charakterze komercyjnym z załącznikami o dużej objętości (zidentyfikowano 323 takie wiadomości). Znacząca liczba maili typu spam poświęcona była usługom finansowym, w tym: kredytom, pożyczkom czy też ofertom „szybkiej gotówki". Badania pokazują, że w strukturze zebranego spamu dominują jednak wiadomości związane z reklamą rozmaitych produktów i usług (promocje, wyprzedaże, rabaty, okazje, tab. 1). Wybrane z nich mają charakter komercyjny, aczkolwiek bliżej niezidentyfikowany, np. o tytule: „Re: Nadal nie milionerem?" (w treści wątpliwy odnośnik), lub „Czy widzę sztylet przed sobą, zwrócony ku mojej dłoni rękojeścią?" (reklama sklepu z militariami). W grupie niechcianych wiadomości wyróżniają się również te poświęcone ofertom pracy, ubezpieczeń, egzekwowania odszkodowań i windykacji.

Metoda identyfikacji treści maili po słowach kluczowych (przeszukiwanie maili) pozwoliła zakwalifikować do określonej grupy jedynie 22,7% zebranych wiadomości.

[20] Security Response, op.cit.

Metoda w obecnym kształcie wymaga więc znacznego rozszerzenia słów kluczowych przypisanych danej kategorii oraz takiego skonfigurowania aplikacji przeszukującej treść spamu, aby wiadomości opisane kilkoma słowami kluczowymi nie były wielokrotnie zaliczane do jednej i tej samej kategorii bądź też nie były zaliczane do kilku kategorii jednocześnie.

Tabela 1

Słowa kluczowe wykorzystane w identyfikacji treści zawartych w badanych wiadomościach typu spam

Treść wiadomości typu spam (Spam content types)	**Konto służbowe**	**Konto prywatne**
Edukacja – kursy, szkolenia, konferencje, język	323	81
Moda, outlet, fashion	18	50
Reklama produktów i usług – promocje, wyprzedaże, sklep, zakupy, rabat	666	566
Kampanie społeczne, pomoc dla…	5	3
Oferty finansowe – kredyty, pożyczki, szybka gotówka, bank	696	315
Ubezpieczenia, odszkodowania, windykacja	120	74
Zdrowie, uroda, leczenie, odchudzanie, dieta, sport	23	41
Sieci społecznościowe	150	46
Praca, zatrudnienie, zarabiaj, zawód	19	222
Phishing	123	78
Inne wiadomości śmieci	7760	4570
Razem	9903	6046

Źródło: Badania własne.

Spam często oznaczany jest wykrzyknikiem (wysoki priorytet), często też do wiadomości dołączane są pliki różnego rodzaju. Zdarza się to zarówno w mailach reklamowych, jak i phishingowych. Jedną z praktyk spammingowych jest rozpoczynanie nagłówka wiadomości przyimkiem „Re:", który oznacza „w odpowiedzi na list", co ma sugerować odbiorcy, że jest to dalszy etap prowadzonej już korespondencji.

Spam jest nie tylko uciążliwy i bywa niebezpieczny dla użytkowników. Badania pokazują, że wielkość maili wynoszących nawet kilka megabajtów stanowi w skali globalnej poważne obciążenie serwerów. Tylko na jednym koncie pocztowym, założonym w jednym z ogólnopolskich portali internetowych, w badanym okresie zebrano 6046 maili w formie spamu, które zajmowały ponad 130 MB przestrzeni dysku serwera (tab. 2). Największa wiadomość mailowa będąca spamem, którą odnotowano w badaniach, zajmowała 10 MB. Całość spamu zebrana w okresie badań, w ramach służbowego konta pocztowego zajmowała ponad 560 MB przestrzeni dysku serwera. Biorąc pod uwagę liczbę kont pocztowych w skali całej firmy, wnioskować można, że spam pochłania duże zasoby pamięci i mocy obliczeniowej serwerów. Wnioskować można również, że jeżeli w okresie około 1,5 roku, w ramach jedynie 2 skrzynek pocztowych, zebrano około 700 MB (pojemność płyty CD-ROM) niechcianych wiadomości, to skala spamu jest w świecie ogromna.

Tabela 2

Objętość maili typu spam w stosunku do ich liczby

Rodzaj wiadomości	Objętość i liczba maili			
	Konto służbowe		Konto prywatne	
	Objętość maili (MB)	Liczba maili	Objętość maili (MB)	Liczba maili
Spam phishingowy	42,7	123	18,4	78
Pozostały spam	518,0	9780	111,7	5968
Łącznie	560,7	9903	130,1	6046
Średnia objętość spamu phishingowego (KB)	347		236	
Przeciętna objętość wiadomości spam (KB)	56,6		21,5	

Źródło: Badania własne.

Niechcianym wiadomościom często towarzyszą różnorakie załączniki. To one stanowią o objętości maila. Niepokojący jest fakt, że większość wiadomości o objętości powyżej 1 MB odnotowano na koncie służbowym (tab. 3). Wynika to z faktu, że przyjęło ono więcej spamu w postaci ofert handlowych i usługowych, którym często towarzyszyły załączniki, formularze, foldery itp. W skali całej zebranej korespondencji przeważają jednak maile tekstowe, których wartość informacyjna jest zwykle dla przeciętnego użytkownika zerowa.

Tabela 3

Badany spam z uwagi na wielkość wiadomości

Przyjęta skala	Liczba maili	
	Konto służbowe	Konto prywatne
> 1 MB	78	8
500-1000 KB	62	12
100-499 KB	615	181
2-99 KB	8623	4345
1 KB	525	1500
Liczba maili łącznie	9903	6046

Źródło: Badania własne.

Niechciane wiadomości rozsyłane w zautomatyzowany sposób i stanowiące potencjalne zagrożenie dla odbiorcy przyjmowały zróżnicowaną formę. W okresie, w którym prowadzono badania, odnotowano 10 wiadomości stanowiących bezpośrednią próbę wyłudzenia danych autoryzacji dostępu do kont bankowych lub kont pocztowych (tab. 4). Zidentyfikowano również aż 96 prób wyłudzenia danych do kont pocztowych, z czego znakomita większość dotyczyła konta służbowego. W tym miejscu należy podkreślić, że maile phishingowe miały zwykle globalny charakter i trafiały na wiele skrzynek pocztowych jednocześnie. Kolejnym zjawiskiem niebezpiecznym były maile z załącznikami w postaci różnorakich plików, których otwarcie powodowało zainfekowanie komputera złośliwym oprogramowaniem. Maile te przyjmowały postać „zaczepną", mniej lub bardziej spersonalizowaną i zawierały bezpośrednie zwroty mające na celu nakłonić odbiorcę do

otwarcia załącznika. Inne z kolei były tak zredagowane, aby wzbudzić ciekawość lub niepokój.

Tabela 4

Odnotowane formy ataków z wykorzystaniem spamu

Phishing	**Konto służbowe**	**Konto prywatne**
– bankowy	5	5
– konto pocztowe	82	14
– wyłudzenie środków finansowych „na zły regulamin”	1	1
– oszustwo na wygraną w loterii, konkursie itp.	3	20
Próba infekcji złośliwym oprogramowaniem	32	50
Łącznie	123	78

Źródło: Badania własne.

Ataki phishingowe odnotowane w eksperymencie przeprowadzane były z kont pocztowych rejestrowanych w domenach narodowych całego świata. W badaniach zidentyfikowano spam z domen rosyjskich (ru), czeskich (cz), rumuńskich (ro), włoskich (it), hiszpańskich (es), niemieckich (de), malawijskich (mw), filipińskich (ph), wenezuelskich (ve), brazylijskich (br), tunezyjskich (tn), chilijskich (cl) oraz innych, jak np. domeny biz, com czy pl. Świadczy to o tym, że spam nie zna granic terytorialnych, ma zasięg globalny, a ataki phishingowe są zwykle przeprowadzane w zautomatyzowany sposób, z zagranicznych kont, co może utrudnić identyfikację sprawcy.

Swoistą odmianą spamu jest ten, na który godzi się użytkownik, zakładający nieodpłatną skrzynkę pocztową. Reklamy internetowe wyświetlane w strukturze witryny oraz te rozsyłane mailem są ceną, jaką musi ponieść użytkownik za bezpłatne korzystanie z adresu.

W ocenie badacza trudno jest porównywać konta e-mailowe, które wykorzystano w badaniu, ponieważ mnogość i złożoność czynników, które wpływają na liczbę odbieranych wiadomości spamowych, jest zbyt duża. Warunkują to między innymi: zabiegi administratorów systemu pocztowego i jego oprogramowanie, forma udostępniania adresu e-mailowego na stronach internetowych oraz liczba i charakter witryn, które ten adres udostępniają, wiek adresu pocztowego, sposób korzystania ze skrzynki pocztowej i wiele innych. Badania pokazują jednak, że konto firmowe przyjęło więcej spamu, który stanowił znacznie częściej próbę wyłudzenia danych autoryzacji dostępu do skrzynki pocztowej. W zakresie obydwóch skrzynek odnotowano liczne próby zainfekowania komputera złośliwym oprogramowaniem. Świadczyć to może o tym, że konta firmowe mogą być przez oszustów preferowane, zwłaszcza w przypadku mniejszych podmiotów rynkowych, instytucji państwowych lub placówek oświaty.

Różnice w strukturze maili mogą wynikać z wielu czynników, w tym z rodzaju zabezpieczeń stosowanych przez administratorów, również z konfiguracji własnej użytkownika oraz sposobu odbierania maili (za pomocą formularza internetowego lub klienta

poczty). Przeprowadzony audyt pozwolił zidentyfikować problemy, z których do najistotniejszych zaliczono:

1. Prostą konstrukcję adresów mailowych i tworzenie wszystkich na podstawie jednego klucza.
2. Zjawisko umieszczania adresów mailowych na witrynach służbowych za pomocą znacznika HTML „mailto". W żargonie twórców witryn internetowych jest to określane mianem „smażenia adresów mailowych, czy też smażenia maili". Tak udostępniany adres jest narażony na aplikacje sieciowe, które w zautomatyzowany sposób tworzą bazy adresów, odczytując je bezpośrednio z kodu witryny przez identyfikację wskazanego znacznika.
3. Częste przypadki udostępniania danych autoryzacji dostępu do poczty przez pracowników.
4. Wykorzystywanie służbowego adresu pocztowego w celach prywatnych.
5. Brak kontaktu z działem informatyki w przypadku wątpliwości względem otrzymanej wiadomości pocztowej.
6. Częste zapisywanie haseł w pamięci przeglądarki lub klienta poczty.
7. Częste przypadki utraty hasła.
8. Brak systemu wymuszającego regularną zmianę hasła do skrzynki pocztowej.
9. Brak szkoleń, niewiedzę, niepewność i nieumiejętność korzystania z firmowych skrzynek pocztowych.

6. Zalecenia służące zwiększeniu ochrony przed spamem

Przeciętny użytkownik nie jest zorientowany w kwestiach technicznych związanych z działaniem serwera poczty. Interesuje go nieskomplikowana aplikacja sieciowa, która umożliwi sprawne odbieranie i wysyłanie wiadomości, załączanie plików oraz zautomatyzowane tworzenie bazy adresów. Zabiegi działu informatyki powinny być więc nakierowane na edukowanie personelu w zakresie właściwego posługiwania się adresem e-mailowym tak, aby nie trafił on do bazy adresowej spamu. W gestii personelu technicznego jest zadbanie o właściwą konfigurację i obsługę systemu pocztowego oraz o poprawne umieszczanie adresów na stronach internetowych.

Aby zapobiegać otrzymywaniu wiadomości typu spam, zaleca się:

1. szanowanie adresu służbowego i rozwagę przy jego udostępnianiu. Należy unikać publikowania adresu na stronach grup dyskusyjnych, forach, czatach oraz w innych obszarach publicznych Internetu. Zabronione są rejestracje internetowe poczynione w celach prywatnych na podstawie służbowych adresów mailowych,

2. stosować zasadę ograniczonego zaufania w stosunku do otrzymywanych wiadomości pocztowych, telefonicznych oraz otwieranych stron internetowych,
3. w przypadku każdej wiadomości budzącej wątpliwości sprawdzać jej nagłówek i weryfikować adres pocztowy nadawcy. Większość niechcianych wiadomości, które stanowią próbę wyłudzenia danych bądź też zainfekowania komputera złośliwym oprogramowaniem jest wysyłana ze skradzionych lub specjalnie do tego celu utworzonych kont pocztowych. W wybranych przypadkach pomocna może być bezpośrednia weryfikacja nadawcy maila,
4. jeżeli pojawi się potrzeba podania adresu mailowego w witrynie internetowej, zaleca się sprawdzenie obowiązujących tam zasad zachowania poufności informacji i ochrony danych osobowych, w szczególności aspektów ujawniania adresów e-mail innym podmiotom. Nie zaleca się rejestracji w niezaufanych serwisach,
5. nie odpowiadać na niechciane wiadomości. Na podstawie odpowiedzi nadawca uzyska potwierdzenie, że dany adres pocztowy jest aktywny i można go dalej wykorzystywać w procederze spamowania. Frazy „zrezygnuj z subskrypcji, zrezygnuj z powiadomienia" często stanowią sposób, w jaki oszuści weryfikują aktywne adresy mailowe. W ten sposób liczba niechcianych wiadomości może się zwiększyć,
6. ze względów bezpieczeństwa nie należy korzystać z odsyłaczy (linków) zawartych w wiadomościach z niepewnego źródła. Tak rozsyłane linki mogą prowadzić do zainfekowanych witryn,
7. administratorom serwisów internetowych czy też redaktorom treści zaleca się unikanie zamieszczania na ich stronach adresów mailowych w formie otwartej, tj. po zakodowaniu z wykorzystaniem znacznika „mailto". Adresy internetowe publikowane na stronach internetowych można chronić, m.in. przez zakodowanie ich z wykorzystaniem języków skryptowych.

7. Poczynione obserwacje i dyskusja wyników

Badania pokazują, że spam może być nie tylko narzędziem ataku lub źródłem złośliwego oprogramowania, stanowi również poważne obciążenie firmowej infrastruktury sieciowej. Problemu nie rozwiążą limity nakładane na wielkość załączników, które można przyjmować lub też wysyłać. W pewnym sensie do spamu należy podchodzić indywidualnie. Użytkownicy poczty internetowej mają różne skrzynki pocztowe, różne upodobania i mogą mieć różne wyobrażenie spamu. Co więcej, zabezpieczenia antyspamowe mogą działać tak, że jako spam oznaczane mogą być wiadomości, których odbiorca oczekuje. Stąd też problemu mogą nie rozwiązać również filtry antyspamowe. Limity objętości skrzynek

pocztowych są koniecznością, ale trudno jest je blokować, w momencie gdy są przepełnione. Praktyka pokazuje, że każdorazowo jest to interpretowane jako swoista „ingerencja w wolność" i wiąże się ze sprzeciwem, czy wręcz oburzeniem użytkowników, którzy są zwykle przekonani, że limity danych ich nie obowiązują, a regularne porządkowanie wiadomości ich nie dotyczy. Należy również pamiętać, że administratorzy firmowych kont pocztowych nie są upoważnieni do usuwania jakiejkolwiek korespondencji pracowników. Serwery są więc przeciążone, aplikacja obsługująca pocztę spowalnia, pracownicy są niezadowoleni z poczty i koło się zamyka. Wszystko to przemawia za regularnymi szkoleniami i nieustannym przypominaniem użytkownikom o potrzebie usuwania nieaktualnych lub niepotrzebnych już wiadomości.

Analiza spamu pokazuje również, że skrzynki służbowe są znacznie częściej zaśmiecane dużymi wiadomościami, które często są rozszerzane o załączniki w postaci ofert handlowych, wzorów umów, zaproszeń, zapowiedzi, materiałów reklamowych i wielu innych. Wszystko to pokazuje, jak trudne zadanie leży po stronie administratorów poczty, którzy muszą tak ją skonfigurować, aby wszystkie „właściwe maile" docierały do użytkowników, a jednocześnie blokowana była jak największa liczba wiadomości śmieci.

Znakomita większość wiadomości to typowe śmieci, o wątpliwej treści. Pojawia się więc pytanie, czemu w ogóle służy ich rozsyłanie, jeżeli nie mają one na celu wyłudzenie danych i są zwykle poświęcone reklamie wątpliwych produktów i usług? Fakt, że tego typu spam jest wciąż w obiegu, świadczy, że przynosi oszustom wymierne korzyści, np. w postaci maili zwrotnych z prośbą o zaprzestanie dalszego spamowania. Wysłanie prośby tego typu stanowi potwierdzenie dla oszustów, że dany mail jest aktywny i przyczyni się do jeszcze większej liczby odbieranych wiadomości śmieci.

W trakcie użytkowania skrzynek pocztowych objętych monitoringiem zauważono, że im starszy adres internetowy, tym więcej odbiera niechcianych wiadomości. Świadczy to o tym, że raz przechwycony przez aplikacje spamowe e-mail jest następnie przekazywany dalej i znaleźć się może w bazach adresowych wielu spamerów.

Same wiadomości typu spam wytwarzają swoisty statyczny szum informacyjny. Mają przede wszystkim charakter natrętny, który wynika głównie z dużej liczby wiadomości, które spływają na skrzynki pocztowe. Sam w sobie przeciętny spam jest niegroźny, ale uciążliwy. Wzbudza znużenie i zażenowanie użytkowników, którzy każdego dnia zmuszeni są do mozolnego przedzierania się przez dziesiątki wiadomości śmieci, a oprogramowanie filtrujące bywa zawodne. Do filtrów antyspamowych często trafiają wiadomości, które nie powinny się tam znaleźć.

Duża liczba wiadomości śmieci sprawia, że większość użytkowników poczty elektronicznej w ogóle takich maili nie przegląda, nie analizuje treści, natychmiast usuwa. Wszystko to sprawia, że struktura spamu się zmienia. Oszuści wykorzystują socjotechniki

służące wyłudzeniu danych bądź też infekowaniu urządzeń z dostępem do Internetu – komputera, telefonu czy też tabletu. Wiadomości są często redagowane tak, aby zaciekawić użytkownika treścią. W tym celu stosowane są niedopowiedzenia, bezpośrednie zwroty i zachęty, np. odwołujące się do poczucia obowiązku, wzbudzające wątpliwości, np. „nasza umowa w załączeniu", „zaległa faktura do pobrania", „zostałeś sfotografowany", „próba doręczenia przesyłki". Częstą praktyką jest dołączanie do wiadomości załączników.

Po rozmowach z pracownikami z pokolenia Millennials (26-34 lata) można odnieść wrażenie, że spam nie robi na nich żadnego wrażenia. Jest on dla jego przedstawicieli tak naturalny jak korzystanie z poczty internetowej. Pokolenie to zdaje się być również znacznie bardziej odporne na działania oszustów od swoich starszych kolegów. Nie stanowi to jednak reguły. W większości przypadków atakom phishingowym ulegają osoby o pewnych cechach charakterologicznych, przy zaistnieniu dogodnych okoliczności. Wszystko to sprawia, że w niedalekiej przyszłości możemy się spodziewać nowych form oszustw internetowych z wykorzystaniem spamu, przez co niezbędny jest stały monitoring zagrożenia i organizowanie regularnych szkoleń z zakresu zagrożeń informacji i infrastruktury teleinformatycznej.

8. Podsumowanie

Wraz z pojawieniem się Internetu pojawiły się zagrożenia na polu jego użytkowania. W dobie powszechnej cyfryzacji i otwartego dostępu do technik i narzędzi komputerowych, w szczególności programistycznych, nie sztuką jest przeprowadzić atak phishingowy. Sztuką jest tak go przeprowadzić, aby nie zostać zidentyfikowanym w sieci i złapanym. Stąd też w Internecie wiele jest wiadomości spamowych stanowiących potencjalne zagrożenie dla użytkownika, jednak w większości mają one niedoskonały charakter i można je w prosty sposób rozpoznać, przez co uniknąć zagrożenia.

Wynikiem przeprowadzonych badań i poczynionych obserwacji są materiały edukacyjne, które posłużyły jako podstawa do realizacji cyklu szkoleń z zakresu ochrony przed spamem, przeprowadzonych wśród pracowników firmy, w której przeprowadzono audyt bezpieczeństwa danych. Szkolenia spotkały się z dużym zainteresowaniem i uznaniem pracowników, którzy brali w nich udział.

Przeprowadzony audyt wykazał pewną barierę kontaktu pomiędzy działem informatyki a szeregowymi pracownikami, którzy zwracali uwagę na swoisty brak wsparcia informatycznego, brak wskazówek i szkoleń branżowych. W audytowanej firmie kładziono nacisk na bezpieczeństwo i ochronę danych, ale nie szkolono pracowników, jak o to

bezpieczeństwo dbać. Szkolenia były więc odpowiedzią na zapotrzebowanie, które zgłaszali pracownicy. Stały się również elementem ocieplania wizerunku działu informatyki.

Walka z zagrożeniami płynącymi ze spamu oraz z samym spamem powinna być prowadzona dwutorowo i równolegle – odgórnie, zarówno od strony technicznej, informatycznej przez stosowny personel działu informatyki, jak i przez odpowiednie wytyczne, procedury, instrukcje i szkolenia prowadzone dla pracowników przez kadrę menedżerów; oddolnie – profilaktyka oraz uwaga pracowników w codziennej pracy z danymi, w tym w pracy z adresami mailowymi, ze szczególną dbałością o ich właściwe udostępnianie i raportowanie o potencjalnych próbach oszustwa.

Bibliografia

1. Brzostowski T.: Innowacje, technologie, zagrożenia w świecie XXI wieku – z perspektywy finansów. Alterum, Warszawa 2012.
2. Bukowska E., Filipowska A., Abramowicz W.: Zapewnienie bezpieczeństwa przez semantyczne monitorowanie cyberprzestrzeni. „E-mentor", nr 3 (50), 2013.
3. Chełstowski D., Szewczyk A.: Problemy rozwoju handlu elektronicznego w Polsce. Zeszyty Naukowe. Studia Informatica, nr 30. Uniwersytet Szczeciński, Szczecin 2012.
4. Crawford M., Khoshgoftaar T. M., Prusa J. D., Richter A. N., Al Najada H.: Survey of review spam detection using machine learning techniques. "Journal of Big Data", Vol. 2(1), 2015.
5. Czyżak M.: Spamming i jego karalność w polskim systemie prawnym. „Pomiary, Automatyka, Kontrola", nr 55, 2009.
6. Gostomski E., Michałowski T.: Rola Internetu w handlu międzynarodowym. „Współczesna Gospodarka", nr 5(3), 2014.
7. ITU, The World in 2014: ICT Facts and Figures, International Telecommunication Union (ITU 2015), www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf, 10.12.2015.
8. Kos-Łabędowicz J., Talar S.: Rola internetu w procesie zmian międzynarodowych stosunków gospodarczych. „Studia Ekonomiczne", nr 218, 2015.
9. Król K.: Organizacyjne aspekty zarządzania bezpieczeństwem danych z perspektywy zagrożeń phishingu. „Organizacja i Zarządzanie", nr 2(30), 2015.
10. Maik A.: Ochrona przed spamem w przepisach. „Folia Bibliologica", nr 57, 2015.
11. Miller P.: Wprowadzenie do obserwacji online: warianty i ograniczenia techniki badawczej. „Przegląd Socjologii Jakościowej", nr 1, 2012.

12. Pekao, Najważniejsze zasady, których warto przestrzegać, płacąc online. Biuletyn Bezpieczny Internet. Luty 2015, https://www.pekao24.pl/MCP/client/logon/bi_pdf/SafeInternet022015.pdf, 03.12.2015.
13. Security Response, Symantec Security Response – malware, security risks, vulnerabilities, and spam, http://www.symantec.com/security_response/landing/spam, 01.12.2015.
14. Symantec, The 2015 Internet Security Threat Report from Symantec, Vol. 20, April 2015, www.symantec.com/security_response/publications/threatreport.jsp, 01.12.2015.
15. Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka F.: Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia. KNF, Warszawa 2010.
16. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną. Dz.U. 2002 Nr 144, poz. 1204.
17. Waglowski P.: Spam w formie niezamówionej informacji handlowej jako delikt nieuczciwej konkurencji, [w:] Tubielewicz A. (red.): Problemy informatyki w zarządzaniu. Politechnika Gdańska, Gdańsk 2003.