CBKE
e-BIULETYN

SPAM – metody walki i obrony

Mariusz Mikoś

student piątego roku zaocznych studiów prawa, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

Internet jest bardzo obszernym źródłem informacji, pozwala na komunikowanie się w najbardziej wszechstronny sposób z wieloma użytkownikami, umożliwia wykorzystanie uzyskiwanych tą drogą informacji w celach zarówno naukowych i komercyjnych. Obok tych niewątpliwych zalet istnieją również wady i niedogodności. Jedną z nich jest spam.

Skala zjawiska jest znaczna. Liczby które są podawane przez firmy i organizacje badające ruch sieciowy, są zatrważające: 73% maili to spam (wg. Message Labs), a koszty to 25 mld USD (wg. International Telecomunication Union, która szacuje poziom spamu nawet na 80%).[1]

„Elektroniczna wiadomość jest spamem, jeżeli:

1. treść i kontekst wiadomości są niezależne od tożsamości odbiorcy, ponieważ ta sama treść może być skierowana do wielu innych potencjalnych odbiorców,

oraz

2. jej odbiorca nie wyraził uprzedniej, możliwej do weryfikacji, zamierzonej, wyraźnej i zawsze odwoływalnej zgody na otrzymanie tej wiadomości,

oraz

3. treść wiadomości daje odbiorcy podstawę do przypuszczeń, iż nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z jej odebrania."[2]

Ad(1) Spammerzy często zmieniają treści wysyłanych listów, a wpływ na to mają kroki prawne i faktyczne skierowane przez ich przeciwników. Niezamówioną przesyłką jest zatem nie tylko oferta formułowana wprost („zamów towar u nas w niewiarygodnie niskiej cenie"), ale także

[1] Dane za Spam & Spyware, Enter Special 1/2005
[2] oryginalne tłumaczenie http://nospam-pl.net/standard , strona dostępna dnia 26.01.2005r.

fikcyjne listy do przyjaciół, w którym informuje się o przypadkowym znalezieniu atrakcyjnej oferty.

Ad(2) Zgoda odbiorcy musi być wyrażona przed wysłaniem reklamowego listu, a nie w formie zapytania zawartego w e-mailu, które to jest tylko pretekstem mającym posłużyć za usprawiedliwienie działalności spammera. Możliwość weryfikacji ma zapewne przybierać formę umożliwienia wglądu do danych przez osoby, których one bezpośrednio dotyczą. Zgoda nie może być domniemana, adresatowi powinna przysługiwać forma rezygnacji z dalszego otrzymywania wiadomości z tego źródła.

Ad(3) W tym zakresie mieści się zjawisko masowego wysyłania jednakowych w treści listów, w dodatku z serwerów, do których dostęp został uzyskany w sposób cyberprzestępstwa. Odbiorca wykorzystujący pocztę np. do pracy, a zmuszony podstępem (np. tematem listu „ważna sprawa") do odbioru poczty zawierającej np.: grafikę, zdjęcia (o objętości przekraczającej zawsze zwykły list w formacie tekstowym) narażony jest na zbędne koszty.

Najpopularniejsze rodzaje spamu:

a) „Hoax"[3] - jest to żart, łańcuszek szczęścia (lub nieszczęścia), forma bardzo popularna i wykorzystująca naiwność (ktoś daje coś za darmo) lub okazanie pomocy przez rozesłanie wiadomości do znajomych (pomoc choremu). W ostatnim czasie bardzo popularne stało się „informowanie" o zagrożeniu ze strony fikcyjnego wirusa. Zwykle ktoś wpada na pomysł fałszywego alarmu („ten plik to wirus" – podając nazwę mniej znanego pliku systemowego), gorzej, gdy w liście zawarty jest link do „szczepionki", która na pewno nie uratuje systemu. Dodatkowo spammer otrzymuje potwierdzenie, że odbieramy i czytamy spam.

b) Reklamy – niewielki koszt dotarcia do potencjalnych klientów. Co prawda, skuteczność „spammerów" nie jest imponująca, gdyż mierzona poprzez ilość otrzymanych odpowiedzi nie przekracza 1%, to zachęca niewielkimi nakładami (wysyła się miliony takich e-maili reklamowych jednocześnie).

c) „Nigeryjski szwindel" – adresat otrzymuje propozycje udziału w przetransferowaniu majątku w wielkich rozmiarach (np. 50 mln. dolarów USD). Istnieje przy tym potrzeba wpłaty kilkuset dolarów na koszty łapówek, czy sfałszowanie dokumentów. Zwykle adresaci traktują to jako żart, jest to bardzo niebezpieczny sposób na wyciąganie coraz to większych sum od zaślepionych żądzą dużego zarobku.

d) „Joe-job" – wrogami ludzi wysyłających nie zamówione przesyłki są twórcy serwisów edukujących użytkowników internetu w kwestii spamu. Ukrywając się pod ich nazwiskami i adresami, spammerzy rozsyłają ankiety lub linki do usuwania swojego adresu z list spammerów.

[3] Wszystkie określenia rodzajów spamu za http://nospam-pl.net , strona dostępna dnia 26.01.2005r.

Zamiast spokoju, w skrzynce lądują jeszcze większe ilości e-maili, gdyż zostaliśmy właśnie się do kolejnych list adresowych.

Spam pomaga w rozwoju i rozprzestrzenianiu się innym procederom sieciowym. Wysyłanie dużej ilości przesyłek pocztowych może posłużyć do ataków mailbombing, wspiera rozprzestrzenianie wirusów i robaków internetowych. Często dzieje się tak, że złośliwe mikroby wykorzystują komputer i konto pocztowe zarażonego użytkownika do rozsyłania swoich kopii.

Pośrednio związanym zagrożeniem jest phishing, czyli wyłudzanie numerów kont i haseł w bankach internetowych. Użytkownik otrzymuje przesyłkę, w której informuje się, że trzeba koniecznie odwiedzić witrynę banku w bardzo ważnym celu - pod pretekstem konieczności zmiany haseł, sprawdzenia poprawności działania systemu. Podany w liście link prowadzi zwykle do strony o podobnym do bankowego adresie (lub następuje trudne do spostrzeżenia przekierowanie). Przestępstwo to ułatwia lenistwo użytkowników, którym nie chce się własnoręczne wpisać adres banku w przeglądarce i sprawdzić otrzymanych informacji, a także dziury w programach (np. Internet Explorer pozwalał sprytnie ukryć fakt przekierowania na inną stronę w sytuacji, gdy w oknie adresowym widniał prawdziwy adres banku).

Także spoofing korzysta z natłoku sieciowych śmieci. Polega na ukrywaniu prawdziwego adresu nadawcy przez jego sfałszowanie. Z jednej stronie wysyłający masową korespondencję reklamową – spammerzy wykorzystują spoofing do ukrywania się przed organami ścigania, a z drugiej mogą podszyć się pod konkretnego adresata i w ten sposób wydobyć istotną informację, nawet taką stanowiącą tajemnicę zawodową, osobistą lub handlową.

Aby przeciwdziałać spamowi, trzeba postawić pytanie: jak w jaki sposób działają osoby nazywane „spammerami" ? Zasad jest kilka, wszystkie wiążą się z ochroną naszego adresu pocztowego.

Po pierwsze, należy wybrać sobie, o ile to możliwe, oryginalną nazwę użytkownika, czyli login. Aby utrudnić wykorzystanie automatów do tworzenia potencjalnych adresów należy unikać adresów łatwych do wygenerowania np.: andrzejw-, andrzejb-czy andrzejc@wp.pl.

Po drugie, wykorzystywanie innego konta pocztowego do wypełniania ankiet i formularzy na stronach WWW. Unikanie promocji i konkursów, które budzą wątpliwości, a także rozsądne korzystanie z ofert darmowych ściągnięć plików czy innych usług świadczonych w zamian za podanie adresu e-mail.

Po trzecie, należy ukrywać adres przy korzystaniu z grup dyskusyjnych. Można zamaskować adres za pomocą dopisanego ciągu znaków, który wskazuje w jasny sposób na jego zbędność (np. georgie@pocztaBLEBLE.pl). Specjalistyczne serwisy poświęcone edukacji antyspamowej (np. http://nospam-pl.net) przytaczają inne sposoby np. oddzielanie składników

adresu za pomocą kilku spacji. Pozostawienie niezmodyfikowanego w w/w sposób adresu grozi bardzo szybkim przyrostem listów oferujących usługi, które zwykle nie są internaucie potrzebne.

Po czwarte, na własnych stronach internetowych nie wolno przedstawiać adresu pocztowego w sposób jawny. Można posłużyć się „trikiem", wewnątrz kodu html, odwracającym adres w lustrzanym odbiciu. Gdy odwiedzający będzie chciał do nas napisać w polu adresat Do: pojawi się już właściwy adres mailowy. Innym sposobem jest umieszczenie obrazka z naniesionym adresem w programie graficznym.

Dodatkowo, można nieco zdeformować obrazek, aby oszukać automaty do wyszukiwania adresów w zasobach www. Warto wiedzieć, że przeszukiwana jest nie tylko warstwa strony internetowej, którą widzimy na ekranie, ale także jej zapis w postaci kodu html (nie wystarczy na stronie WWW wpis „napisz do mnie", gdyż adres i tak musi znaleźć się „wewnątrz strony" poprzedzony wpisem mailto.

Inny sposób proponuje Center for Democracy & Technology[4]: należy adres mailowy zapisać w formie kodów ASCII, które zostaną przetłumaczone przez język HTML na formę zrozumiałą dla człowieka.

Po piąte, „należy zwracać uwagę na zaznaczone domyślnie opcje przy wypełnianiu formularzy w celu skorzystania z internetowych kont czy usług. Mogą być tam opcje dot. otrzymywania e-maili innych towarów lub usług."[5]

Podejmowanie działań w obronie niezakłóconego korzystania z poczty elektronicznej w pierwszej kolejności należy do osoby zainteresowanej. W tym celu należy zatem:

1. Sprawdzić, czy dostawca usługi e-mail udostępnia opcje antyspamowe i odpowiednio skonfigurować filtry z uwzględnieniem czarnych i białych list oraz nauki filtrów poprzez wskazanie przesyłek nie chcianych i tych pożądanych. W razie potrzeby zastosować aplikację do filtrowania poczty na komputerze lokalnym.
2. Zmienić program pocztowy - jeśli nie umożliwia stosowania filtrów, rozdzielania przesyłek za pomocą zdefiniowanych szablonów.
3. Wyłączyć obsługę wyświetlania emaili w formacie html – należy tylko pozostawić obsługę przesyłek w formacie tekstowym – aby nie wysyłać potwierdzenia aktywności konta do spammerów. W żadnym razie nie wolno odpowiadać na przesyłki zawierające informacje o możliwości wykasowania własnego adresu z bazy adresowej poprzez list o tytule UNSUBSCRIBE. Łukasz Kozicki, autor serwisu NOspamPL, radzi, aby nie wypisywać się z list do których samemu się nie zapisywało. Nie ma bowiem żadnej gwarancji,

[4] http://www.cdt.org
[5] htttp://us-cert.org – Cyber Security Tip ST04-007

że adres rzeczywiście zostanie wykasowany. Nawet gdyby tak się stało, nasz adres, jako potwierdzony, może zostać sprzedany do bazy adresów innemu spammerowi.

4. Zablokować usługę Posłaniec/Messenger w systemie Windows NT/2k/XP, aby uniemożliwić wysyłanie spamu za pomocą komendy systemowej *net send* na nasz adres IP.

W odpowiedzi na lawinowy wzrost skali spammingu podjęto faktyczne działania obronne. W pierwszej kolejności zaczęto dbać o bezpieczeństwo użytkowników kont poczty elektronicznej. Usługi antyspamowe pojawiły się najwcześniej w zakresie usług świadczonych odpłatnie. W następnej kolejności uruchamiano taką ochronę dla kont darmowych, najpierw czasowo
(np. poczta.onet.pl), potem na stałe. Automaty oddzielające spam stanowią obecnie standard w ofercie najpopularniejszych portali w Polsce (Onet, Interia, o2, wp czy Gazeta). Istnieje także oprogramowanie pomagające w filtrowaniu poczty przychodzącej na konto pocztowe, w formie oddzielnych aplikacji plug-inów do popularnych programów pocztowych.

Kolejnym krokiem powinno być zgłaszanie przypadków spamu do CERT Polska (Computer Emergency Response Team). Wiadomość powinna być przesłana w formie załącznika na adres spam@cert.pl w ciągu 48 godzin od wysłania.[6]

O skali problemu świadczy szereg kroków podejmowanych przez władze, które miałyby na celu ograniczenie zjawiska. Od 01.01.2004 r. W Stanach Zjednoczonych obowiązuje Can-Spam Act (Controlling the Assault of Non Solicited Pornography And Marketing Act). Jednak opinie o jego skuteczności, po upływie roku, nie są zbyt optymistyczne. Firmy zajmujące się badaniem zjawiska niechcianej poczty alarmują, że udział spamu w poczcie elektronicznej osiągnął już 60-70% i będzie stale rósł[7]. Dzieje się tak pomimo wysokich kar, z karą więzienia włącznie. Ciężar procesowania się przejęły na siebie stanowe instytucje sprawiedliwości oraz dostawcy internetu.

W lecie 2004 r. OECD powołała grupę zadaniową zajmującą się zjawiskiem spamu.

W Polsce także zajęto się prawnym uregulowaniem problemu. Znalazło to wydźwięk w uchwaleniu 18.07.2002 r. ustawy o świadczeniu usług drogą elektroniczną. Według art. 10 ust. 1 „Zakazane jest przesyłanie niezamówionej informacji handlowej skierowanej do oznaczonego odbiorcy za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej."[8]

[6] http://www.cert.pl/index3.html?id=12, strona dostępna 26.01.2005r.
[7] Grant Gross „Is CAN SPAM working?", http://www.pcworld.com.
[8] Art.10.1 ustawy o świadczeniu usług drogą elektroniczną, Dz.U. z dn. 9 września 2002 r nr.144 poz1204 z późn. zmianami.

Opisane wyżej działanie stanowi czyn nieuczciwej konkurencji w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (art. 10 ust. 3).

W ustawie znalazła się definicja informacji handlowej zawarta w art. 2 ust. 2 – jest to *każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku*. Wyłączone zostały informacje *nie służące osiągnięciu efektu handlowego*. Zatem poza regulacją pozostały przesyłki będące tak denerwującymi fałszywymi alarmami, żartami, łańcuszkami szczęścia.

Za rozsyłanie *niezamówionej informacji handlowej* przewidziano karę grzywny w wysokości do 5000 zł, przy czym uzależniono ściganie tego wykroczenia od wniosku pokrzywdzonego (art. 24 ust.1 i 2).

Andrzej Adamski wskazuje na istotne ograniczenie zastosowania ustawy, gdyż „ma ono [spam – dop. MM] bowiem swoje źródła głównie w Stanach Zjednoczonych AP, skąd wychodzi w świat, na ogół pod fikcyjnym adresem zwrotnym, ok. 85% materiałów reklamowych krążących w Internecie. Ze względu na miejsce działania (zagranica), sprawca czynu określonego w art. 24 ustawy o świadczeniu usług drogą elektroniczną nie podlega polskiej jurysdykcji w sprawach o wykroczenia."[9]

Mimo że od wejścia w życie omawianej tu ustawy mijają już dwa lata, sądy nie zostały zalane pozwami przeciwko spammerom. Prowadzącym serwis vagla.pl[10] udało się w tym czasie znaleźć jeden (!) taki przypadek. Czy jest to tylko skutek braku wiary w sprawność polskiego sądownictwa? Namierzanie domniemanych spammerów jest czasochłonne i kosztowne, przynajmniej w obliczu wątpliwych rezultatów tych poszukiwań (gdy nadawca dobrze się zabezpiecza przed dekonspiracją).

Może traktowanie tego zjawiska jako wykroczenia to zbyt mało, szczególnie w odczuciu nieprofesjonalnego prawniczo ogółu społeczeństwa? Tak wiele przecież wykroczeń popełnianych jest nagminnie i nie może doczekać się na skuteczną reakcję organów ścigania? Czy *ustawa o świadczeniu...* podzieli los przepisów nakazujących właścicielom sprzątanie po ich czworonożnych pupilach?

Z drugiej strony grzywna do 5000 zł może być karą dostatecznie dotkliwą. A pozostaje jeszcze droga cywilna dla poszkodowanych. Traktowanie spammingu jako przestępstwa zagrożonego np. karą pozbawienia wolności nie byłoby zbyt racjonalne.

[9] A.Adamski, Karnoprawna ochrona dziecka w sieci Internet, Prok.i Pr. 2003/9/59 t.-3.
[10] http://www.vagla.pl.

Moim zdaniem rozwiązanie omawianego problemu może przyjść z całkiem innej strony. Szerokie omawianie zagrożeń w prasie i mediach elektronicznych na pewno spowoduje wzrost świadomości i chęć zabezpieczenia się przed zaśmieceniem swojego konta. W edukacji użytkowników widzę realną i naprawdę skuteczną barierę dla spammerów. Przestrzeganie zasad i nieznaczna modyfikacja dotychczasowych zachowań będzie stale zmniejszać atrakcyjność tej drogi marketingu.

Nie jest w stanie tego zburzyć nawet kontrofensywa w postaci nowych „trików" omijających istniejące zabezpieczenia.

W sukurs zwykłym internautom już idą dostawcy usług internetowych, którzy darmowo udostępniają filtry antyspamowe. Tanieją także konta komercyjne.

Administratorzy zostali zmuszenie do poprawienia poziomu zabezpieczeń (na serwerach pracują programy, które można przecież poprawić!). Wystarczy przypomnieć, że jeszcze 5-6 lat temu wysłanie poczty, nawet tej „seryjnej", z pomocą usługi telnet nie stanowiło większego problemu.

Kolejnym, ale nie ostatnim, ośrodkiem walki stała się społeczność sieciowa, czyli wszyscy użytkownicy „dobrej woli". Idea i działanie czarnych list spammerów także odegra istotną rolę w przezwyciężeniu zalewu śmieci.

Uporządkowanie sytuacji na wszystkich tych poziomach (od internauty do wielkich dostawców dostępu) zminimalizuje zagrożenie spamem do poziomu „nieuciążliwości". Będzie ono zatem istniało dopóty, dopóki będą chętni na ich wykorzystanie. Przy wykazaniu, że jest to popularny sposób dotarcia do potencjalnych klientów stron oferujących treści erotyczne, można uznać przyszłość spamu za pewną.

Prawo nie pozostanie pewnie w tyle. Świadczy o tym kolejny oręż w postaci art. 172 ust. 1 ustawy Prawo telekomunikacyjne. Zakazuje on używania w marketingu bezpośrednim *automatycznych systemów wywołujących* bez wcześniejszej zgody abonenta. Może on zatem obejmować sytuacje wykorzystywania skryptów, które bez udziału operatora masowo wysyłają spam.

Zasady netykiety, szczególnie w sytuacjach, gdy znalazły one swoje odbicie w konkretnych punktach umów o świadczenie usług przyłączeniowych, także mogą pomóc. Stanie się to z korzyścią dla konieczności znajomości standardów zachowania i niewątpliwie ukontentuje najstarszych stażem użytkowników.

Ze spamem warto walczyć. Koszty, które za sobą pociąga, to nie tylko te, które da się łatwo wyliczyć (jak czas stracony na żmudne usuwanie śmieci ze skrzynki pocztowej zamiast poświęcony na rzeczywistą pracę, czy zbędne obciążanie sieci przesyłowych i marnotrawienie

czasu pracy serwerów), ale także koszty społeczne. Nie zamówiona poczta może zniechęcać do formy elektronicznych listów, a nawet obniżać zaufanie do e-maili. Powstawać może konieczność wymagania dodatkowego, tradycyjnego (np. w drodze kosztownych połączeń telefonicznych) potwierdzania otrzymywania przesyłek dot. wyjątkowo ważnych spraw.

Szczególnie godny potępienia jest fakt, iż tylko dla swojego zysku spammer potrafi bez wahania zaśmiecić setki czy tysiące kont pocztowych za pomocą przysłowiowego jednego „kliknięcia" myszą!

Użytkownik nie pozostaje bezbronny i o tym musi on wiedzieć i pamiętać. Powinien zacząć bronić się sam: czy to zmieniając program pocztowy, dotychczasowe zwyczaje ujawniania swojego adresu w sieci, albo korzystać z ochrony antyspamowej już na poziomie serwera pocztowego. Na ile użyteczne są przepisy prawa, okaże się po obserwacji działań powołanych organów (rzecznicy konsumenta) i orzeczeń sądów, które zapadną w sprawach o spamming. Ich reakcja jest bardzo istotna, aby przepisy prawa nie stały się tylko zapisami wynikającymi z ogólnoświatowej mody na prawną walkę ze spamem. Muszą one być prawnym wsparciem dla działań faktycznych.

Literatura:

1. Spam & Spyware, Enter Special, 1/2005
2. Paweł Rożyński, Zrób to spam, Gazeta Wyborcza z 24.01.2005 r.
3. http://nospam-pl.net wraz z podstronami, dostępna 26.01.2005 r.
4. http://www.us-cert.org wraz z podstronami, dostępna 26.01.2005 r.
5. http://www.pcworld.com wraz z podstronami, dostępna 26.01.2005 r.
6. http://www.cert.pl wraz z podstronami, dostępna 26.01.2005 r.
7. http://www.cdt.org wraz z podstronami, dostępna 26.01.2005 r.