Magdalena Ziobrowska, Piotr Ziobrowski

Anonimowy e-mail : zagrożenia dla biznesu

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 2, 85-91

2009

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

Magdalena ZIOBROWSKA
Piotr ZIOBROWSKI
Gnieźnieńska Wyższa Szkoła Humanistyczno-Menedżerska „Milenium"

ANONIMOWY E-MAIL – ZAGROŻENIA DLA BIZNESU

Wprowadzenie

W społeczeństwie współczesnym zarządzanie firmą, korporacją, czy instytucją jest możliwe dzięki informacji. „Informacja jest w gospodarce wolnorynkowej kluczowym elementem warunkującym sukcesem – to ona jest podstawą podejmowania decyzji".[1] Warto jednak pamiętać, że niemal każdego dnia spotykamy się z nadmiarem informacji. Często docierają do nas informacje, które niekoniecznie są do nas adresowane np. w postaci reklam. Z pojęciem informacji wiąże się pojęcie komunikacji. Komunikacja personalna jest „przekazem treści między jej ludzkimi uczestnikami, który to proces buduje wspólnotę".[2] W dzisiejszym społeczeństwie „scenę komunikacji społecznej cechuje bogactwo środków przekazu (gesty, sygnały, znaki pozawerbalne, tekst drukowany, komunikacja telefoniczna, wiadomości MMS)".[3] „Instrumentami, które ze względu na możliwość szybkiego kontaktu z docelowymi klientami oraz relatywnie niskie koszty zrewolucjonizowały komunikację marketingową, są Internet oraz technologie mobilne".[4] „Internet może być skutecznie wykorzystywany w technikach marketingu bezpośredniego".[5] Większości z nas, z Internetem nieodzownie kojarzy się poczta elektroniczna. „Używana do komunikowania się z przyjaciółmi, rodzina, współpracownikami, stała się narzędziem powszechnego użytku na uczelniach, w instytucjach rządowych, korporacjach przemysłowych i domach".[6] Poczta elektroniczna jest bardzo często wykorzystywana w marketingu. Tanim i wydawałoby się skutecznym sposobem na marketing jest wysyłanie reklam w postaci e-maili. Warto podkreślić, iż obecnie sposób ten jest stanowczo nadużywany. Współczesny użytkownik Internetu widząc emaila z reklamą automatycznie traktuje go jako spam. Nawet jeśli jest to firma, z którą kontaktu sobie wcześniej zażyczył. P. Majewski pisze: „Dzisiaj ludzie, którzy codziennie korzystają z e-maila, codziennie otrzymują wiele nowych wiadomości. Osobiście codziennie dostaję nawet 100 e-maili – po przejrzeniu ich przez asystenta i usunięci ponad 1000 maili ze spamem przez filtr antyspamowy".[7] Dobrodziejstwa emaili doprowadziły do masowego rozsyłania spamu. Sprzyjają temu programy typu anonimizujące. W swej idei stworzone w celu zapobiegania inwigilacji. W poniższym tekście, chcielibyśmy zwrócić uwagę, że programy te, mają wiele niekorzystnych dla ogółu użytkowników Internetu funkcji i zastosowań.

---

[1] R. Wawrowski: *Sprawozdawczość finansowa źródłem informacji o przedsiębiorstwie*. W: A. Kamela-Sowińska (red.): *Gospodarka a społeczeństwo informacyjne.* Poznań 2008, s. 187
[2] J. Mikułowski-Pomorski: *Jak narody porozumiewają się ze sobą w komunikacji międzykulturowej i komunikowaniu medialnym.* Kraków 2006, s. 23
[3] M. Iwanowska-Maćkowiak: *Europa on-line. Elektroniczne formy informowania dostępne w Unii Europejskiej*. „Zeszyt Naukowy Wyższej Szkoły Ekonomii i Innowacji" Lublin 2006, nr 2, s. 79
[4] M. Ankiel-Homa, T. Olejniczak: *Komunikacja z klientem w społeczeństwie informacyjnym*. W:. A. Kamela-Sowińska, op. cit., s. 17
[5] S. Sleight: Sukces w e-biznecie. *Poradnik menedżera.* Warszawa 2002
6 P. Wallach: Psychologia Internetu. Poznań 2004, s. 12
[7] P. Majewski: *Czas na e-biznes. Jak myślisz, ile można zarobić na stronie WWW*? Gliwice 2007, s. 214

Anonimowość w Internecie

Problem anonimowości w Internecie jest coraz częściej poruszany.[8] „Wraz z rozwojem technologicznym, problem prywatności przybierał w historii ludzkości coraz większe znaczenie. W okresie, kiedy głównymi środkami wymiany informacji były bezpośredni przekaz ustny czy też tradycyjnie realizowany przekaz w postaci pisma ręcznego a następnie druku, wystarczającym elementem ochrony prywatności były rozwijane w okresie średniowiecza normy etyczne. W miarę rozwoju technologii wymiany informacji oraz wzrostu znaczenia jej posiadania, normy etyczne zastąpiono formalnie obowiązującymi przepisami prawa. Szybki rozwój technologii informatycznej w drugiej połowie XX wieku sprawił jednak, że zarówno normy etyczne jak i formalnie obowiązujące przepisy prawa, stały się niewystarczające. Dla skutecznej ochrony prywatności we współczesnym świecie, niezbędne stało się również stosowanie odpowiednich środków technicznych."[9] Pamiętać bowiem musimy, że „każdy pakiet wysyłany przez nasz komputer do Internetu może ostatecznie posłużyć do wyśledzenia nas".[10] „Sieć Internet, której początki sięgają lat 60-tych (ARPANET), tworzona była początkowo spontanicznie w ośrodkach naukowych i akademickich. Przy formułowaniu tych fundamentów nie przywiązywano szczególnej wagi do bezpieczeństwa – nie przewidywano, że użytkownicy sieci mogą mieć względem siebie nieuczciwe intencje. Sieć miała pomagać w wymianie wyników badań czy spostrzeżeń naukowych. Dzisiaj rozwój infrastruktury Internetu jest głównie domeną prywatnych firm. Pole zastosowań sieci przybrało również nową postać, w której udział przedsięwzięć komercyjnych zajmuje jedną z dominujących ról. System WWW (World Wide Web) stanowi w tych przemianach podstawowy czynnik".[11]

Poczta elektroniczna

Często wysyłając maila myślimy, że kontaktujemy się z w sposób anonimowy. Faktem jest, że na pierwszy rzut oka nie jesteśmy w stanie nic o tym emailu powiedzieć ale zaglądając w głąb niewinny emaila powie nam bardzo dużo. W jego nagłówku zawarte są wszelkie informacje typu kto, kiedy i skąd go wysłał. Nie oszukamy pracodawcy że leżymy chorzy w łóżku a w rzeczywistości jesteśmy na wakacjach. W sieci znajdziemy proste serwisy umożliwiające takie czynności z których każdy nawet średnio zaawansowany użytkownik Internetu może skorzystać, nie mówiąc już o odpowiednich służbach które mając dostęp do danych zawartych na serwerach naszego dostawcy Internetu, będą mogły stwierdzić z jakiego komputera wysłaliśmy maila, a nie tylko jak szef, że piszemy z Poznania.

Anonimowy e-mail daje możliwość wysyłania tekstu bez możliwości identyfikacji nadawcy lub podszycia się pod konkretny login. Może to powodować dezinformacje. Bardzo istotne znaczenie w tym wypadku jest to, że e-mail staje się niewiarygodny, a wiec powszechnie używany sposób do przekazywania informacji staje się niewiarygodny.

---

[8] Por. M. Ziobrowska: *Anonimowość w Internecie*. W: A. Buczek, D. Czajkowska-Ziobrowska, D. Rondalska, P. Ziobrowski: *Zainteresowania badawcze młodzieży akademickiej*. Poznań 2009. ss. 18-22

[9] http://techinfo.giodo.gov.pl/index.html dnia 10.03.2008

[10] A. Lockhart: 125 sposobów na bezpieczeństwo sieci. Praktyczny przewodnik po technikach zabezpieczania sieci komputerowych. Gliwice 2007, s. 103

[11] http://techinfo.giodo.gov.pl/index.html dnia 10.03.2008

Programy tego typu są dobrodziejstwem w krajach ogarniętych represją takich jak Chiny czy Białoruś. Ale mają też negatywne zastosowanie do podszywania się oszukiwania i rozsyłania spamu.

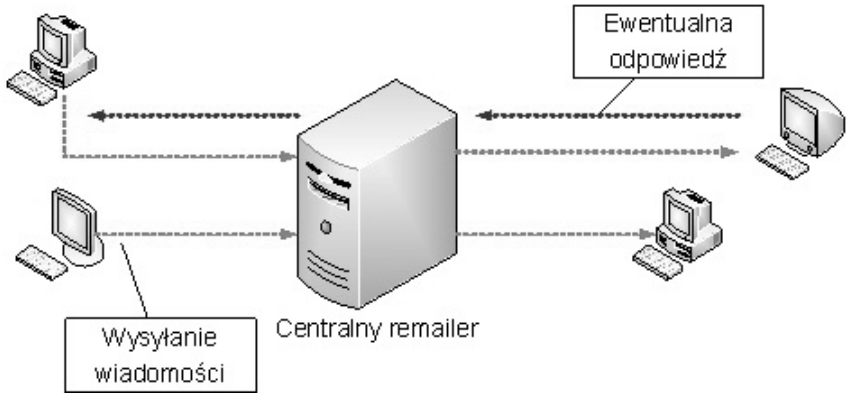
Rysunek nr 1. . Strona internetowa pozwalająca na odczytanie skąd pochodzi e-mail
Źródło: http://www.ip-adress.com/trace_email/

Programy umożliwiające anonimowe wysyłanie e-maili

Historia anonimowego wysyłania e-maili rozpoczęła się w 1993 w Helsinkach. Usługa była dostępna na słynnym serwerze anon.penet.fi. Zasada działania była prosta. Użytkownik wysyłał e-mail na adres Remailer wraz z dołączonym w nagłówku adresem docelowym, następnie serwer przesyłał wiadomość dalej zmieniając nadawcę na cyfry@anon.penet.fi (słowo cyfra zastąpione było losową liczbą)

Podstawową wadą opisanego remailera był fakt że przechowywał on bazę danych z informacjami na temat kto i do kogo wysyłał emaile. Umożliwiało to odpowiedź odbiorcy na otrzymanego email ale jednocześnie stanowiło zagrożenie dla anonimowości użytkownika. Osobie której udało by się dostać do tej bazy posiadała wszystkie informacje i mogła złamać anonimowość każdego użytkownika.

Anonimowość ta mogła zostać również złamana poprzez atakującego dzięki analizie ruchu wchodzącego i wychodzącego z serwera. Praca serwisu zakończyła się konfiskacją serwera przez lokalną prokuraturę.

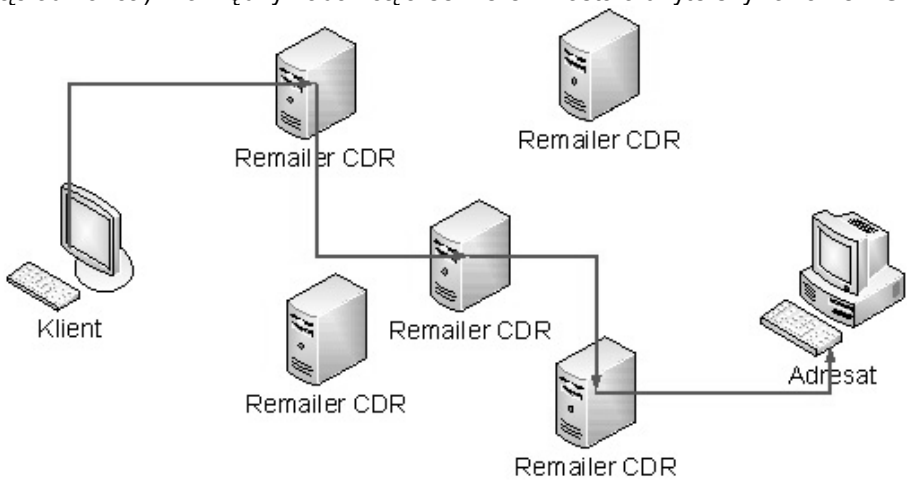


Rysunek nr 2. Schemat działania remailera anon.penet.fi

Bezpieczniejszym remailerem jest jego następca twór grupy CYPERPHUNKS, z uwagi na fakt, że nie korzysta on z jednego centralnego serwera ale wielu rozproszonych. Nazwano je Cypherpunks Distributed Remailer czyli w skrócie CDR.

Przez serwery te kolejno przechodzi wysłany przez użytkownika email w drodze do odbiorcy. Każdy z węzłów w łańcuchu zna tylko swojego poprzednika i następnik, a tylko pierwszy z łańcucha remailerów zna adres rzeczywistego nadawcy. System więc nie przechowuje bezpośrednio danych korzystających z niego użytkowników.

Z technicznego punktu widzenia systemie tym nadawca szyfruje wiadomość kluczem publicznym serwerów przez które kolejno przechodzi wiadomość (zaczynając od końca). Pomiędzy nadawcą a serwerem zostało użyte szyfrowanie PGP.



Rysunek nr 3. Schemat działania remailera Cyberpunk

Każda przesyłana wiadomość miała określony schemat. Rozpoczynała się znakiem " ::" po czym podany był adres docelowego adresata lub kolejnego w ścieżce remailera, właściwa treść wiadomości lub już wcześniej zaszyfrowana

wiadomość podawana była dopiero po pojedynczej pustej linii informującej o zakończeniu nagłówka. W każdej warstwie pojawiała się informacja o szyfrowaniu PGP dla każdego serwera pośredniczącego w wymianie. Klucze PGP tych serwerów pobierane były poprzez wysłanie wiadomości o temacie remailer-keys. Klucze te można było też otrzymać wraz z instrukcją obsługi oraz z informacjami konfiguracyjnymi dla programu Premail, w odpowiedzi na wiadomość o temacie remailer-help.

Takie podejście do przesyłania e-maili stawia już większą trudność w ustaleniu rzeczywistego nadawcy ale w dalszym ciągu nie wymaga to od atakującego zbyt wielkiego wysiłku. Potencjalne formy ataku to analiza wielkości lub kolejności wychodzących i wchodzących pakietów. System nie przewidywał możliwości odpowiedzi na otrzymanego emaila

Następca Cyberphunk był bezpieczniejszy system *MIXMASTER*. Remailer ten skorygował wiele błędów poprzednika. Przez długi czas serwery Mixmaster współpracowały z Cyberpunk W celu uniknięcia możliwości rozpoznania nadawcy wiadomości poprzez korelację czasu remailer ten stosuje opóźnienie w czasie na poszczególnych serwerach. Wiadomość bezpośrednio po otrzymaniu jej przez kolejny serwer nie jest przesyłana do kolejnego węzła lecz czeka do momentu aż zostanie uzbierana odpowiednia grupa wiadomości na danym serwerze, po czym wszystkie grupowo przesyłane są do kolejnego remailera. Ponadto dla zwiększenia bezpieczeństwa program kliencki dzieli wszystkie wiadomości na paczki o stałej wielkości dzięki temu zabiegowi stała się niemożliwa analiza wielkości wiadomości na wejściu oraz wyjściu remailera. Pakiety oznakowane są ID co umożliwia połączenie wiadomości na ostatnim węźle. Jeśli do tego węzła w odpowiednim czasie nie dotrą wszystkie paczki mające się składać na pojedynczą wiadomość, zgromadzone dotychczas paczki są usuwane.

Dla gwarancji dotarcia do odbiorcy paczki mogą zostać wysłana równolegle wieloma ścieżkami, przy czym ostatni z remailerów na ścieżce musi być dla wszystkich tych ścieżek taki sam gdyż jego funkcją jest łączenie paczek w wiadomość oraz usuwanie ewentualnych duplikatów paczek. Ze uwagi na ten fakt nie możliwe jest zalewanie odbiorcy kopiami e-maila poprzez wstawienie wiadomości do łańcucha remailerów. Szyfrowanie stosowane jest na każdym etapie komunikacji w łańcuchu węzłów. W tym przypadku wykorzystany został algorytm symetryczny dla szyfrowania całej wiadomości natomiast nagłówek zawierający klucz jest szyfrowany kluczem publicznym każdego z węzłów uczestniczących w komunikacji. Takie rozwiązanie przyspiesza proces szyfrowania. W przypadku próby odpowiedzi na wiadomość jest ona przesyłana bezpośrednio do ostatniego remailera z którego została otrzymana. W nim jest kodowana kluczem symetrycznym zapisanym w danym węźle i w takiej formie wysłana do kolejnego węzła w łańcuchu, w którym czynność ta się powtarza. Do momentu w którym remailer kontaktujący się z bezpośrednio z autorem wiadomości przekaże mu ją. Po otrzymaniu zostaje ona rozszyfrowana przy użyciu zapisanych uprzednio kluczy symetrycznych. Program kliencki systemu również nosi nazwę Mixmaster. Dostępny jest on zarówno na platformę Windows jak i różne dystrybucje linuxa. Pozwala on użytkownikowi w łatwy sposób wysyłać wiadomości. Daję możliwość samodzielnego lub automatycznego określenia liczby i ścieżki serwerów przekierowujących.

Następny typ remailera to uznawany za bezpieczniejszy program **MIXMINION**, nazywany remailerem 3 generacji. Od swoich poprzedników odróżnia go

przede wszystkim sposób odpowiedzi na otrzymane maile. Pojawił się mechanizm Single Use Reply Block SURB, który likwiduje możliwość rozpoznanie nadawcy poprzez wielokrotną odpowiedź na tego samego email i analizowanie ilości przekazywanych wiadomości przez kolejne remailery. Zarówno e-maile wchodzące jak i wychodzące zachowują ten sam poziom anonimowości. Klienci oraz wierzchołki Mixminion do komunikacji używają bezpiecznych szyfrowanych kanałów opartych na TLS. TLS umożliwia zestawianie tuneli przy użyciu krótko terminowych kluczy symetrycznych ustalanych przy użyciu algorytmu Diffie-Hellmana. Klucz ten jest usuwany po zestawieniu połączenia a po jego zakończeniu generowany jest nowy. Uniemożliwia to odkrycie historii zestawianych połączeń np. przez nakaz sądu lub innych organów. Używanie połączeń typu TLS utrudnia ataki tak jak Man In The Middle czyli ingerencji w przesyłane dane. Dla rozpowszechniana formalnych informacji niezbędnych do tworzenia tuneli czyli Dotyczących dostępnych remailerów, ich obciążenia, kluczy używana jest mała grupa zsynchronizowanych nadmiarowych serwerów.

Rysunek nr 4. Jeden z serwisów pozwalający na wysłanie emaila z innego – sfałszowanego adresu

Źródło: http://www.ehaker.com/anonimowy-email/

Remailer ten jest kompatybilny zarówno z remailerami I jak i II generacji. Kompatybilność w tył jest zapewniona poprzez „remixing” wiadomość pochodzącego od mix mastera w wiadomość typu III.

Internet daje również możliwość nie tylko ukrycia się w globalnej pajęczynie ale również podszycia się pod danego nadawcę. Takie programu znajdziemy w różnych serwisach internetowych.

Podsumowanie

Warunki rozwoju współczesnego biznesu podlegają ciągłym zmianom. W celu pozostania nadal na rynku, zarządzający przedsiębiorstwem, specjaliści od marketingu firmy, muszą wykazać się szybką na nie reakcją. Internetowa eksplozja wybuchła jakiś czas temu i ciągle w niezwykłym tempie się rozwija. Korzystanie z Internetu dla większości nie stanowi już problemu w codziennym jego wykorzystywaniu. Większość internautów korzysta z poczty elektronicznej. Wspomniany środek komunikacji wykorzystywany jest niemal w każdym biznesie. Z reguły dostrzegamy tylko pozytywne strony wysyłania i odbierania e-maili. Warto jednak pamiętać, iż e-maile mogą stanowić zagrożenie dla biznesu.