WYBRANE KIERUNKI ZABEZPIECZEŃ W SYSTEMACH MARKETINGU ELEKTRONICZNEGO

Tomasz Turek
Politechnika Częstochowska, Polska

Streszczenie

Artykuł odnosi się do zagadnień ochrony danych w systemach informatycznych marketingu (SIM). Wyróżniono podstawowe elementy sytemu, wskazano potencjalne zagrożenia oraz metody zabezpieczeń. W ten sposób przedstawiono zarys metody inwentaryzacyjnej jaką stosuje się do ochrony systemów informatycznych.

Wprowadzenie

Prowadzenie działalności gospodarczej przy wykorzystaniu systemów informatycznych stało się zjawiskiem powszechnym. Dzięki systemom informatycznym można znaleźć kontrahentów, dokonać transakcji kupna-sprzedaży, a następnie ją rozliczyć w sposób elektroniczny. Innym przykładem wykorzystywania systemów informatycznych jest tworzenie tzw. wirtualnych stanowisk pracy. Polega to na tym, że zatrudniony pracownik pracuje w własnym miejscu zamieszkania, a wyniki swej pracy przesyła drogą elektroniczną i w ten sam sposób jest również rozliczany.

W efekcie systemy informatyczne stają się nośnikami rzeczywistych procesów gospodarczych (czasami nawet jedynymi, jak w przypadku procesów wirtualnych). W tej sytuacji nie dziwi fakt konieczności tworzenia odpowiednich systemów zabezpieczeń. Zabezpieczenia te muszą chronić systemy informatyczne i ich zasoby przed możliwością ich zniszczenia lub uszkodzenia w sposób przypadkowy, na skutek zdarzeń losowych, a także przed świadomą agresją.

Celem niniejszego artykułu jest wskazanie wybranych metod zabezpieczeń, jakie są stosowane w systemach informatycznych marketingu.

1. Charakterystyka marketingu elektronicznego

Marketing elektroniczny oznacza prowadzenie działalności ekonomicznej przy wykorzystaniu sieci rozległych np. Internetu. Począwszy od nawiązania i budowania wzajemnych relacji między podmiotami gospodarczymi, a skończywszy na usługach posprzedażnych i ponowieniu raz już przeprowadzonej transakcji. Jego zastosowania to między innymi (3):

- poszukiwanie klientów i potencjalnych partnerów handlowych przy zastosowaniu sieci;
- marketing towarów i usług przez prezentację ich walorów potencjalnym użytkownikom przy wykorzystaniu między innymi WWW, poczty elektronicznej i grup dyskusyjnych;
- bezpośrednia sprzedaż wszelkiego rodzaju dóbr konsumpcyjnych i usług;
- handel wirtualny np. zakup i sprzedaż akcji;
- badania rynkowe dokonywane za pomocą poczty elektronicznej;
- obsługa gwarancyjna i pogwarancyjna klientów prowadzona przez sieć;

- zarządzanie sieciami dystrybucyjnymi i handlowymi – wspieranie dystrybutorów dealerów, sprzedawców tworząc ponadorganizacyjne jednostki prowadzące sklepy wirtualne.

2. Uczestnicy procesu

Uczestnikami procesów marketingowych wspieranych za pomocą usług informatycznych może być wiele rodzajów organizacji. Zaliczyć można do nich między innymi:

- przedsiębiorstwa produkcyjne, handlowe lub usługowe, które pragną zdynamizować swoją działalność marketingową za pomocą usług teleinformatycznych lub organizacje wirtualne czyli tzw. sklepy i przedsiębiorstwa internetowe;
- dostawcy usług internetowych – są to przedsiębiorstwa, które pomagają w realizacji idei marketingu elektronicznego;
- instytucje finansowe obsługujące elektroniczną działalność gospodarczą.

Pomiędzy uczestnikami elektronicznego procesu marketingowego zachodzą relacje wykorzystujące usługi teleinformatyczne dostępne w sieciach rozległych. Przedsiębiorstwo chcące zaistnieć w Internecie i prowadzić za jego pomocą działalność marketingową, zanim nawiąże jakikolwiek kontakt z klientem musi określić zakres i formę wykorzystania sieci komputerowych jako medium komunikacji ze swoimi partnerami gospodarczymi. Chodzi o utworzenie serwisu WWW, przedstawiającego firmę w sposób kompleksowy, zawierający informacje o przedsiębiorstwie, jego ofertę cenową etc. Poza tym należy uruchomić adres E-mail, za pomocą którego inni użytkownicy Internetu będą mogli przysyłać informacje. Najczęściej te zadania leżą w gestii dostawcy usług internetowych. Trzeba zwrócić uwagę że tzw. provider pełni tylko rolę wspomagającą przepływy informacyjne lecz nie uczestniczy jako podmiot w procesach marketingowych. Aktywnymi uczestnikami elektronicznych procesów gospodarczych stają się natomiast banki. Bardzo duża liczba instytucji finansowych wprowadziła serwisy sieciowe stymulując w ten sposób również rozwój marketingu elektronicznego. Pomiędzy przedsiębiorstwem a klientem poza wymianą informacji za pomocą usług sieciowych WWW i E-mail następuje coraz częściej elektroniczna obsługa relacji finansowych.

3. Możliwe zagrożenia w systemach marketingu elektronicznego

Każda informacja znajdująca się w przedsiębiorstwie oraz przesyłana za pomocą usług sieciowych jest narażona na różnorakie zagrożenia. Dotyczy to również informacji marketingowych. Zagrożenia te dzieli się na cztery podstawowe grupy (1):

- **kradzież** – kiedy informacja jest przywłaszczana przez intruza; dotyczy do sytuacji kiedy informacja jest kradziona z nośnika pamięci zewnętrznej lub podczas przesyłu siecią;
- **modyfikacja** – kiedy intruz wprowadza nieautoryzowaną zmianę w jej treści;
- **podejrzenie** – kiedy informacja nie jest zmieniona ani skradziona, lecz jej treść jest znana osobom, lub instytucjom do tego niepowołanym;
- **blokada** – w tej sytuacji intruz fizycznie uniemożliwia skorzystanie ze sprzętu komputerowego lub infrastruktury sieciowej.

W systemach marketingu elektronicznego ochrona powinna dotyczyć miejsc przechowywania informacji czyli:

- nośników pamięci komputerów w sieciach przedsiębiorstw,
- serwerów WWW,
- w listach E-mail.

Tam też potencjalni intruzi będą poszukiwać luk oraz innych możliwości ataku. Dlatego też należy stosować odpowiednią politykę ochrony informacji.

4. Metody ochrony

Metody ochrony informacji dzieli się na dwie grupy:

- personalne,
- systemowe.

Pierwsze polegają na fizycznym oddzieleniu osób niepowołanych od sprzętu komputerowego oraz mediów transmisji, dzięki którym odbywa się przesyłanie informacji. Należy więc tworzyć tzw. obszary ochronne. Powinny one być tak stworzone, aby uwzględniały zabezpieczenie przedsiębiorstwa przed fizycznym dostępem osób niepowołanych oraz podsłuchem stosowanym za pomocą różnych technik. Strefy ochronne mają maksymalnie opóźnić dotarcie intruza do obiektu chronionego. Na granicach stref ochronnych stosuje się szereg zabezpieczeń: oznaczenie granicy, informowanie, utrudnianie przejścia i kontrolowanie, monitorowanie i aktywny alarm przekroczenia granicy (2, str. 49).

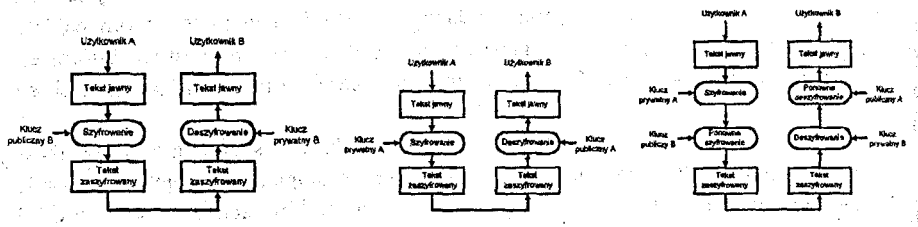
Do grupy zabezpieczeń systemowych zalicza się zabezpieczenia związane z programowym zabezpieczeniem systemu informatycznego. Podstawowe zasady administracyjne dotyczą (2):

- stosowania oprogramowania antywirusowego – jest to konieczne zabezpieczenie informacji przed różnego typu wirusami komputerowymi, dlatego też zakup pakietu antywirusowego powinien być włączony do polityki bezpieczeństwa informacji przedsiębiorstwa; dodać należy, iż nie można ograniczać się tylko do jednego pakietu antywirusowego,
- wykonywania kopii zapasowych zasobów systemowych, a w szczególności nośników pamięci; administrator sprzętu wraz z osobami obsługującymi oprogramowanie powinien ustalić okres, po którym będzie wykonywana archiwizacja istotnych danych i systemu;
- wykorzystywania podstawowych usług zabezpieczających sieć komputerową: **identyfikacji** - za pomocą identyfikatora użytkownika (ID); **uwierzytelnienia** – weryfikacji tożsamości za pomocą hasła, **autoryzacji** – przydzielenie praw dostępu np. do czytania danego pliku i dokonywania w nim zmian, **kontroli dostępu** – nadzorowanie praw dostępu do sieci;
- stosowania zabezpieczeń połączeń sieci komputerowych przedsiębiorstw z sieciami rozległymi; chodzi o tzw. ściany ogniowe (firewall), które przechwytują każdą wiadomość i określa czy pakiet danych lub żądanie połączenia powinno być przepuszczone, czy też nie.

Stosowanie powyższych zabezpieczeń w dużym stopniu eliminuje niebezpieczeństwo ataku na stacje robocze oraz serwery WWW. Jeżeli obsługa serwisu WWW została zlecona tzw. providerowi, to zabezpieczenia pozostają w jego gestii.Pozostaje jeszcze problem bezpieczeństwa informacji przesyłanej drogą elektroniczną pomiędzy klientem a przedsiębiorstwem. Można stwierdzić, iż do tego celu wykorzystuje się głównie pocztę elektroniczną, która może być nośnikiem wielu różnego typu zdarzeń gospodarczych. Powstaje więc pytanie: skąd brać pewność, że dana informacja została przysłana przez zaanonsowaną w niej osobę (jednostkę gospodarczą), lub też, że jej treść nie została zmieniona? Do zabezpieczeń poczty elektronicznej pomocne są metody kryptograficzne, które zamieniają tzw. tekst jawny za pomocą klucza kryptograficznego na zaszyfrowaną wersję zwaną kryptogramem. Obecnie wykorzystuje się dwie podstawowe metody kryptograficzne różniące się od siebie typem zastosowanych kluczy. Są to metody bazujące na algorytmach symetrycznych i asymetrycznych.

W metodach bazujących na algorytmach symetrycznych klucz do szyfrowania i deszyfrowania jest ten sam. Ewentualnie jeden łatwo wyprowadzalny z drugiego.

Z kolei w metodach wykorzystujących algorytmy asymetryczne klucze do szyfrowania i deszyfrowania są różne. Praktycznie nie powinno być możliwe wyprowadzenie jednego z nich z drugiego. Każdy użytkownik posiada dwa klucze: prywatny znany tylko jemu oraz klucz publiczny dostępny dla każdego. Klucze publiczne przedsiębiorstwa mogą publikować na swoich witrynach internetowych. Ta metoda ma dwie ważne cechy. Po pierwsze, praktycznie nie jest możliwe obliczyć klucz deszyfrujący. Po drugie, istnieją metody, w których dowolny z dwóch kluczy może być użyty do szyfrowania, zaś klucz pozostały do deszyfrowania. Dzięki temu można używać klucza prywatnego i publicznego zarówno do szyfrowania jak i do uwierzytelnienia. Przedstawia to poniższy rysunek.



a) utajnianie b) uwierzytelnianie c) utajnianie i uwierzytelnianie

Rysunek 1 a,b,c: Utajnianie i uwierzytelnianie wiadomości za pomocą klucza publicznego

Źródło: (1, str. 59)

Zakończenie

W niniejszych rozważaniach zaprezentowane wybrane metody zabezpieczania systemów informatycznych przed różnymi rodzajami agresji elektronicznej. Skoncentrowano się tu głównie na zabezpieczeniach, które powinny być stosowane w systemach informatycznych marketingu. W tym celu przedstawiono charakterystyczne

elementy SIM oraz starano się przedstawić stosowane w nich zabezpieczenia. Jest to inwentaryzacyjna metoda tworzenia strategii zabezpieczeń stosowanych w systemach informatycznych. W praktyce gospodarczej podobne inwentaryzacje metod zabezpieczeń są opracowywane na zasadzie przeciwstawienia ich do potencjalnych kierunków agresji. Ma to na celu zapobieganie wszelkim możliwościom agresji na zasadzie ex ante lub przynajmniej ograniczanie jej skutków. O tym jak istotna jest to problematyka świadczy prowadzenie szeregu różnego typu badań w zakresie prezentowanej tutaj tematyki.

Literatura:

1. Ahuja V., Bezpieczeństwo w sieciach, Academic Press, 1997
2. Kifner T., Polityka bezpieczeństwa i ochrony informacji, Wydawnictwo Helion, 1999
3. Pańkowski L., Marketing elektroniczny, www.icu.com.pl, 2000

LOKALNY RYNEK USŁUG LINGWISTYCZNYCH W OBLICZU ZMIAN OTOCZENIA MARKETINGOWEGO

Jolanta Urbańska
Politechnika Częstochowska, Polska

Streszczenie

Artykuł jest próbą analizy porównawczej działalności trzech największych na rynku lokalnym konkurentów w dziedzinie świadczenia usług lingwistycznych. Żaden z badanych podmiotów nie posiada zdecydowanej przewagi rynkowej. Natomiast dążenia integracyjne Polski z Unią Europejską stwarzają dla tego placówek nowe możliwości i wyzwania.

Jednym z trendów ostatnich lat jest niezwykle silny rozwój sektora usług. Usługa jest dowolnym działaniem, jakie jedna strona może zaoferować stronie drugiej. Wynik tego działania jest nie prowadzi do nabycia prawa własności, a jego produkcja może być związana lub nie z produktem fizycznym (Kotler Ph., 1999).

Branże usługowe są bardzo zróżnicowane. Sektor usługowy obejmuje zarówno usługi konsumpcyjne, tzw. usługi dla ludności, jak i usługi nabywane przez instytucje, do których zaliczamy: usługi produkcyjne i usługi inwestycyjne. Do sektora usług zalicza się również sektor rządowy obejmujący sądy, biura zatrudnienia, szpitale, policję, straż pożarną, pocztę i szkoły. Do grupy tej zalicza się również instytucje typu non – profit: uniwersytety, muzea, organizacje dobroczynne. Dużą część sfery usług zajmuj sektor biznesu: banki, hotele, linie lotnicze, firmy ubezpieczeniowe.

W przeciwieństwie do innych sektorów specyfika marketingu usług nie jest związana z odmiennością potrzeb i zachowań nabywców, lecz z naturą samych usług jako podstawowego elementu usługowej kompozycji instrumentów marketingowych. Naturę tę określają charakterystyczne cechy usług: niematerialność, nierozłączność, oraz brak możliwości przechowywania.