PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1086 — 2005
Modele i metody zarządzania informacją i wiedzą

Teresa Ciesielczyk i Grażyna Watras
Akademia Ekonomiczna we Wrocławiu

BEZPIECZEŃSTWO HANDLU ELEKTRONICZNEGO

1. Wstęp

Rozwój handlu elektronicznego daje nowe możliwości zarówno przedsiębiorstwom handlowym, jak i ich klientom. Koniecznym warunkiem jest jednak zapewnienie odpowiedniego poziomu zabezpieczenia interesów stron uczestniczących w transakcji handlowej: klienta, sprzedawcy, banku czy instytucji finansowej.

Z badań firmy Symantec [Zwierzchowski 2004, s. C2] wynika, że w pierwszej połowie 2004 r. na świecie najbardziej narażone na ataki były firmy zajmujące się handlem elektronicznym.

Zainteresowanie tą formą działalności cały czas rośnie, choć mogłoby być jeszcze większe, gdyby zapewnione były bezpieczeństwo i prywatność potencjalnych klientów. Nie bez znaczenia jest również zdobycie zaufania klientów do handlu elektronicznego.

Jak wynika z raportów Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) [*Raport...* 2004] oraz firmy Janmedia Interactive [*Raport z badania...* 2004], do handlu elektronicznego można mieć wiele zastrzeżeń. Odnoszą się one do uchybień w informowaniu klientów o ich prawach, głównie chodzi tutaj o kwestie umowy sprzedaży, procedurę gwarancyjną i tryb dochodzenia roszczeń. Na podstawie badań przeprowadzonych przez UOKiK w 186 e-sklepach można stwierdzić wiele nieprawidłowości w budowie i funkcjonowaniu witryny sklepowej, dotyczą one w szczególności braku informacji o [*Raport...* 2004]:

- stosowanych kodeksach etycznych,
- sądzie, który rozstrzygnie ewentualny spór,
- lokalizacji lub danych gospodarczych sklepu,
- języku umowy,
- czasie trwania oferty,

- warunkach reklamacji,
- sposobie korygowania błędów w zamówieniu,
- prawie do odstąpienia od umowy.

Duża część sklepów nie zamieszcza informacji dotyczących ich bezpieczeństwa. Niemal 40% witryn nie zabezpiecza we właściwy sposób danych osobowych konsumentów. W wyniku braku odpowiedniego zabezpieczenia w handlu elektronicznym informacje dotyczące produktów, klientów, transakcji, płatności mogą znaleźć się w rękach konkurencji, oszustów i innych przestępców.

Szczególnie niebezpieczna może się okazać utrata pozytywnego wizerunku e-sklepu, gdzie informacje dotyczące płatności są przesyłane przy wykorzystaniu sieci publicznej. Brak ochrony może pociągnąć za sobą poważne skutki również natury prawnej. W konsekwencji może to być przyczyną znacznej utraty pozycji rynkowej, co w oczywisty sposób pociąga za sobą straty finansowe.

2. Zagrożenia handlu elektronicznego

Przez pojęcie zagrożenia rozumie się potencjalne, negatywne zdarzenia pojedyncze lub grupowe, przypadkowe lub celowe, które mogą spowodować szkody w aplikacji, a także w firmie handlowej.

Biorąc pod uwagę architekturę wraz z jej otoczeniem, zagrożenia można rozpatrywać w dwóch aspektach: technologicznym i wynikającym z organizacji handlu elektronicznego. W aspekcie technologicznym szczególnie narażone na ataki są komunikacja oraz usługi internetowe.

Do zagrożeń wynikających z organizacji handlu elektronicznego można zaliczyć:

- kuszące oferty, w których przedstawiane są duże ilości niedrogich towarów lub drogi towar w atrakcyjnej cenie,
- brak pozytywnych opinii o sprzedających,
- podszywanie się pod witryny znanych sklepów – przez rejestrację pseudoninimów podobnych do nazw, którymi posługują się sprzedawcy o wyrobionej marce,
- brak podstawowych informacji o oferowanych towarach i usługach, a także niejasno oznaczonych cenach,
- brak pełnej informacji o danych adresowych firmy handlowej,
- umieszczanie regulaminów w niejasnych, trudno dostępnych miejscach,
- niejasno sprecyzowana treść regulaminów,
- pomijanie informacji o warunkach i kosztach dostawy,
- brak możliwości korygowania błędów w zamówieniach,
- w ogóle niedostarczenie zakupionego towaru do klienta lub dostawa niepełnowartościowego towaru,
- nieprzestrzeganie wcześniej zadeklarowanych terminów dostawy towaru do klienta,

– brak stałych umów zawartych między e-sklepami a firmami transportowymi (kurierskimi) oraz niestosowanie integracji systemów informatycznych e-sklepów z systemami śledzenia firm kurierskich,

– umieszczanie na stronie w mało widocznym miejscu informacji – „sprzedawca zastrzega sobie możliwość zmiany specyfikacji technicznej" i cen prezentowanych na serwisie produktów oraz umieszczanie informacji „cennik nie stanowi oferty handlowej w rozumieniu prawa",

– brak informacji na temat procedur zwrotu zakupionych towarów,

– posługiwanie się cudzymi kartami kredytowymi przy zakupach *on-line* (2 mln osób w ciągu roku zostało oszukanych na 2,4 mld USD) [*Oszust czyha* 2004, s. 14],

– lekkomyślność klientów polegająca na udostępnianiu swoich danych osobowych przypadkowym osobom [*Uwaga...* 2004, s. 17],

– brak świadomości i wiedzy u projektantów i programistów z zakresu mechanizmów bezpieczeństwa systemów przy tworzeniu aplikacji e-sklepu.

Przedstawione rodzaje zagrożeń mogą spowodować małą wiarygodność witryn sklepowych, kradzież bądź zniekształcenia zasobów informacyjnych handlu elektronicznego, utratę wizerunku firmy handlowej.

3. Zabezpieczenie handlu elektronicznego

Przez pojęcie bezpieczeństwa handlu elektronicznego trzeba rozumieć zbiór procedur, metod i technologii używanych do ochrony usług internetowych, zasobów danych, transakcji płatności oraz dostaw. Bezpieczeństwo w przedstawianym obszarze działań gospodarczych jest związane z:

– etyką postępowania firm handlowych,

– budową zaufania wśród potencjalnych klientów,

– przestrzeganiem przez e-sklepy prywatności klientów,

– przestrzeganiem przepisów prawnych z zakresu e-biznesu.

Cel zabezpieczenia jest spełniony, gdy są zapewnione:

– poufność danych klienta, przejawiająca się w tym, że informacje przez niego podane nie są udostępniane osobom trzecim bez jego zgody,

– potwierdzenie tożsamości klienta pozwalające na udowodnienie, że zamawiający towar jest osobą, za którą się podaje, co jest szczególnie ważne w przypadku dokonywania płatności kartą płatniczą lub transakcji z odroczonym terminem płatności,

– potwierdzenie tożsamości sprzedawcy pozwalające określić, że pod sprzedawcę nikt się nie podszył, że sprzedawca przestrzega zachowanie standardów bezpieczeństwa oraz dba o informacje powierzone mu przez klienta,

– integralność danych pozwalająca na stwierdzenie, że dane (towar, umowa, płatność) przesyłane między partnerami handlowymi docierają do odbiorców w stanie nie naruszonym,

– autoryzacja płatności transakcji wyrażająca się w korzystaniu z pośrednictwa akredytowanych jednostek świadczących usługi certyfikacyjne.

Jak już wspomniano, ważnymi formami zabezpieczeń e-handlu są te, które wynikają z unormowań prawnych. Pozwalają one głównie na uwiarygodnienie stron www i zdobycie zaufania klientów. Istotne są w tym zakresie wymagania następujących ustaw:

– o prawie autorskim i prawach pokrewnych z 4 lutego 1994 r.,
– o ochronie danych osobowych z 29 sierpnia 1997 r.,
– o znakach towarowych z 31 stycznia 1985 r.,
– o zwalczaniu nieuczciwej konkurencji z 16 kwietnia 1993 r.,
– prawo działalności gospodarczej z 19 listopada 1999 r.,
– o ochronie praw konsumentów z 2 marca 2000 r.,
– o świadczeniu usług drogą elektroniczną z 18 lipca 2002 r.

W przedstawianym obszarze istotne jest określenie praw i obowiązków stron zawierających umowę kupna-sprzedaży, co znajduje swój wyraz w ustawie z 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny oraz w niektórych artykułach kodeksu cywilnego (np. art. 66 § 1, art. 71, art. 78, art. 88, art. 70 § 2). Natomiast obowiązek umieszczania na stronach www informacji o siedzibie usługodawcy oraz regulaminu świadczenia usług drogą elektroniczną określa ustawa z 18 lipca 2002 r. Wymóg dotyczący podawania w ofercie danych adresowych wprowadziła także ustawa o działalności gospodarczej.

Istotną kwestią, która może dotyczyć handlu elektronicznego, jest spam. Reguluje to art. 10 ustawy o świadczeniu usług drogą elektroniczną, który zabrania przesyłania nie zamówionej informacji handlowej szczególnie za pomocą poczty elektronicznej, chyba że odbiorca wyrazi zgodę na jej otrzymanie.

Aby zabezpieczyć się przed zarzutem spammingu firma handlowa powinna [Trusiewicz 2004, s. 25]:

– posługiwać się precyzyjnie sformułowaną polityką prywatności opublikowaną na stronach www,
– wymagać, aby każda osoba udostępniająca adres e-mail zgadzała się z treścią polityki prywatności,
– stosować metodę *double opt-in* (adresy na liście są wynikiem prośby ich właścicieli o ich umieszczenie z dodatkowym potwierdzeniem tego zamiaru),
– personalizować mailingi,
– podawać dokładną instrukcję w mailu, jak usunąć adres z listy zgodnie z polityką prywatności,
– umieszczać wszędzie tam, gdzie występuje jakiś kontakt z partnerami zewnętrznymi, skrót polityki prywatności.

W przypadku przesyłania informacji handlowej za zgodą odbiorcy należy dodatkowo wyraźnie ją wyodrębnić i oznaczyć. Musi ona wtedy zawierać [Trusiewicz 2004, s. 26]:

1) oznaczenie podmiotu, na którego zlecenie jest ona rozpowszechniana oraz jego adresy elektroniczne,

2) wyraźny opis form działalności promocyjnej,

3) wszelkie informacje, które mogą mieć wpływ na określenie zakresu odpowiedzialności stron, w szczególności ostrzeżenia i zastrzeżenia.

Zabezpieczenie usług internetowych oraz zasobów danych i komputerów można realizować przez zapory ogniowe i systemy ochrony antywirusowej. Dobrze dobrana zapora ogniowa zabezpiecza całkowicie przed atakami z zewnątrz. Potrafi zapobiec podsłuchowi i podszywaniu się pod uprawnionych użytkowników, blokuje penetrację sieci wewnętrznej, a w zaawansowanych konfiguracjach może chronić przed znanymi wirusami i końmi trojańskimi. Nie zapewnia jednak ochrony przed nowymi wirusami i końmi trojańskimi, nie jest w stanie wykryć elementów, które w chwili instalacji jeszcze nie istniały. Nie zabezpiecza również przed nowymi apletami *Javy* i formantami *ActiveX*. Systemy ochrony antywirusowej muszą w sposób niezawodny rozpoznawać rzeczywiste wirusy i usuwać je, nie uszkadzając przy tym oryginalnych plików. Najnowsze systemy tego typu służą ochronie zarówno serwerów baz danych, jak i poczty elektronicznej. Posiadają zaawansowane mechanizmy wykrywania wirusów zawartych w dokumentach i załącznikach wiadomości e-mail. Skanery działające w tle zabezpieczają pliki zarówno podczas zapisu, jak i odczytu. Wyposażenie tych systemów w mechanizmy aktualizacji oraz powiadomienia o zagrożeniach pozwalają na szybką orientację o grożących niebezpieczeństwach oraz sposobach przeciwdziałania.

Zabezpieczenie przed włamaniami może być realizowane poprzez systemy IDS (*Intrusion Detection System*). Aplikacje te monitorują, wykrywają i reagują na nie autoryzowane działania w sieci w czasie rzeczywistym. Okazuje się jednak, że jest to rozwiązanie niewystarczające, gdyż obecnie ataki są coraz bardziej złożone i przemyślane. Rozwiązaniem w tym zakresie jest uzupełnienie sieciowych IDS hostowymi IDS [Gienas 2004, s. 36]. Pierwsze z nich kontrolują pakiety w sieci pod kątem podejrzanych działań, drugie zaś monitorują anomalie występujące w plikach systemowych, procesach i plikach logów. Pliki logów systemów operacyjnych i aplikacji są przeszukiwane pod kątem znamion szkodliwych działań, system plików jest monitorowany pod kątem penetracji istotnych plików i naruszenia ich zawartości, a ruch sieciowy na okoliczność ataków sieciowych.

Zabezpieczenie komunikacji dotyczy bezpiecznego przesyłania informacji (np. produktu cyfrowego, zamówienia, płatności) przez sieci publiczne z wykorzystaniem szyfrowania, wirtualnych sieci prywatnych VPN i infrastruktury klucza publicznego.

Szyfrowanie jest jednym z najefektywniejszych sposobów zabezpieczenia komunikacji. Oprócz tego ta metoda zabezpieczenia może skutecznie zapobiegać takim zagrożeniom, jak: nieupoważniony dostęp do informacji, podsłuch sieciowy, włamania do systemu, podszywanie się pod inną osobę. Rozwiązanie to może być realizowane programowo lub sprzętowo. W pierwszym przypadku algorytm szy-

frujący, klucze, hasła dostępu itp. znajdują się na dyskach komputera, serwera, co może narazić je na ujawnienie, zniszczenie lub modyfikację. W sprzętowej realizacji wszystkie istotne elementy zabezpieczeń znajdują się w chronionych obszarach urządzenia kryptograficznego, klucze na kartach procesorowych są przechowywane w sprzętowo chronionych obszarach pamięci urządzenia kryptograficznego.

VPN są implementowane jako rozwiązania sprzętowo-programowe lub obecnie częściej programowe. Przez sieć publiczną na bazie Internetu łączy się partnerów handlowych, wyposażając ich w protokół zabezpieczający IPSecurity lub SSL (*Secure Socket Layer*). Pierwszy wymaga instalacji specjalnego oprogramowania na zdalnych stacjach korzystających z zasobów sieci. Stanowi to istotną wadę tego protokółu. Protokół SSL charakteryzuje się dostępnością z poziomu każdej przeglądarki, wysokim poziomem bezpieczeństwa i niewygórowaną ceną.

Infrastruktura klucza publicznego PKI (*Public Key Infostructure*) zapewnia:

– uwierzytelnianie stron oznaczające wiarygodne zidentyfikowanie osób lub systemów, które elektronicznie podpisały wiadomość, umowę lub transakcję,

– weryfikację integralności danych, czyli sprawdzenie, czy przesyłane dane (treść umowy, zlecenie przelewu między kontami, zlecenie wypłaty gotówkowej dla określonej osoby z określonego konta) nie zostały zmienione po ich elektronicznym podpisaniu,

– poufność informacji, czyli pewne szyfrowanie danych przesyłanych między komunikującymi się stronami,

– niezaprzeczalność, czyli niemożność wyparcia się faktu złożenia podpisu (np. pod umową).

Istotą podpisu cyfrowego, opartego na asymetrycznym systemie kodowania, jest wykorzystanie różnych kluczy do podpisu, które pasują wzajemnie do siebie. Dany klucz publiczny może odszyfrować tylko przypisany do niego klucz prywatny. Tym samym klucz prywatny stanowi swego rodzaju pieczęć, która uniemożliwia niedostrzegalną zmianę treści dokumentu i identyfikację dysponenta klucza prywatnego. Instrument certyfikatu zapewnia bezpieczny podpis elektroniczny.

Określone środki bezpieczeństwa powinny być unikatowe dla każdej aplikacji handlu elektronicznego i przestrzegane przez ich partnerów.

4. Podsumowanie

Bezpieczeństwo handlu elektronicznego zależy od bardzo wielu czynników. Ważne jest również, aby każdy klient zdawał sobie sprawę z istnienia i skali potencjalnych zagrożeń z jego strony. Klienci, którzy są tego świadomi, dbają o bezpieczeństwo, stosując następujące zasady:

1) korzystają tylko z sprawdzonych i pewnych komputerów, nigdy z ogólnodostępnych stanowisk,

2) regularnie aktualizują oprogramowanie, ze szczególnym ukierunkowaniem na system operacyjny,

3) stosują aktualne oprogramowanie antywirusowe z możliwością skanowania otwieranych plików i monitorowania wiadomości poczty elektronicznej,

4) odpowiednio konfigurują przeglądarkę z możliwością szyfrowania SSL do 128 bitów,

5) upewniają się, że witryna, na której się logują nie jest jedynie wierną kopią oryginalnego serwisu,

6) wylogowują się po zakończeniu czynności związanych z transakcją lub obsługą konta,

7) przy dodatkowej autoryzacji nie udostępniają numeru karty płatniczej,

8) nie wysyłają poufnych informacji w zwykłej wiadomości e-mail, wybierają tylko pośrednictwo strony www, podczas bezpiecznego połączenia,

9) dokonują zakupów tylko w renomowanych e-sklepach.

Oczywiście nie sposób całkowicie wyeliminować wszystkich oszustw z Internetu. Warto jednak zastosować się do przedstawionych zasad, dzięki czemu można zminimalizować ryzyko korzystania z handlu elektronicznego.

Literatura

Gienas K., *Bezpieczeństwo Internetu*, „Networld" 2004, nr 4.

Oszust czyha, „Enter" 2004, nr 8.

Raport Urzędu Ochrony Konkurencji i Konsumentów o handlu internetowym, Urząd Ochrony Konkurencji i Konsumentów, Departament Polityki Konsumenckiej, Warszawa 2004, http://www.uokik.gov.pl/download/raport%20ecommerce.doc

Raport z badania funkcjonalności polskich sklepów internetowych, Janmedia Interactive 2004. http://www.janmedia.pl/upload/wysiwyg/pdf/report.pdf

Trusiewicz R., *Paragrafem w spam*, „Manager" 2004, nr 3.

Uwaga, złodziej tożsamości, „Internet" 2004, nr 6.

Zwierzchowski Z., *Jak nie haker, to wirus*, „Rzeczpospolita" 13-14 listopada 2004, nr 266.

SECURITY OF E-COMMERCE

Summary

In this article we present some issues concerning security of e-commerce. In the first part we underline technological and organizational threats of this form of business activity. Ways of protection based on both legal and technological security were also discussed.