Zagrożenia procesów komunikacyjnych w e-commerce oraz sposoby przeciwdziałania

BOGDAN KSIĘŻOPOLSKI[1], ZBIGNIEW KOTULSKI[2]

[1]Instutu Fizyki, Uniwersytet Marii Curie-Skłodowskiej
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Polska
[2]Instytut Podstawowych Problemów Techniki PAN
Ul. Świętokrzyska 21, 00-049 Warszawa, Polska, oraz
Instytut Telekomunikacji Politechniki Warszawskiej

1. Społeczeństwo Informacyjne.

Od kilkunastu lat społeczeństwo w jakim się znajdujemy staje się „Społeczeństwem Informacyjnym". Pojęcie „Społeczeństwa Informacyjnego" jest szeroko opisywana w literaturze, trafnym wydaje się być określenie, że „społeczeństwo informacyjne jest etapem w rozwoju cywilizacji, w którym społeczeństwo i gospodarka skoncentrowane są na produkcji, dystrybucji i użytkowaniu informacji; informacja i wiedza stają się podstawowymi czynnikami produkcji" [1].

Jeżeli informacja jest głównym czynnikiem produkcji możemy mówić o nowej gospodarce opartej na zastosowaniu wiedzy a nie na samej produkcji. Jednym z kluczowych elementów który kreuje obraz społeczeństwa informacyjnego jest postęp technologiczny. Rozwój technologiczny przebiega wokół głównych nurtów badań naukowych, od których zależą dalsze przemiany, są to między innymi: sprzęt, oprogramowanie, teleinformatyka.

1.1. Nowa Gospodarka.

W budowanie społeczeństwa informacyjnego zaangażowane jest wiele państw Europy. Powstaje wiele planów oraz inicjatyw, które opisują przeobrażenia oraz założenia dla społeczeństwa informacyjnego. W 2002 roku powstała inicjatywa „eEurope 2005: An information society for all" [2], która bazuje na dwóch głównych grupach aktywności. Pierwsza obejmuje nowoczesne elektroniczne formy usług dla społeczeństwa (e-government, e-lerning, e-health) oraz dynamiczne środowiska dla e-businessu. Druga mówi o infrastrukturze teleinformatycznej oraz zagadnieniach bezpieczeństwa.

Podobne strategie zostały utworzone dla Polski jest nim między innymi „Strategia informatyzacji Rzeczypospolitej Polskiej - ePolska" [3]. Zostały wyodrębnione obszary w obrębie których, projekty mogą zostać zrealizowane. Są to:

- Powszechny dostęp do treści i usług udostępnianych elektronicznie,
- Tworzenie wartościowej oferty treści i usług,
- Zapewnienia warunków ich efektywnego wykorzystania.

Wyodrębniono również projekty, które są krytyczne dla informatyzacji Polski; są to:

- Szerokopasmowy dostęp do Internetu w każdej szkole (Infrastruktura dostępu, bezpieczeństwo sieci),
- „Wrota Polski" (zintegrowana platforma usług administracji publicznej dla społeczeństwa informacyjnego),
- Promocja Polski w Internecie,
- Powszechna edukacja informatyczna.

Część projektów zostało już zrealizowanych, niektóre są w trakcie realizacji. Takimi projektami są np.: eTEN, IDA-II, eContent.

1.2. E-commerce.

Elektroniczna gospodarka obejmuje wiele zagadnień, które często uważane są za tożsame są nimi np.: e-biznes, e-commerce. Chcąc uściślić termin e-commerce możemy przyjąć, że jest to „proces sprzedawania i kupowania produktów i usług, a więc zawierania transakcji handlowych z wykorzystaniem środków elektronicznych, prowadzony za pośrednictwem Internetu" [1]. Aktualnie prowadzonych jest wiele badań w tym zakresie, niektóre są wprowadzane w praktyce. Wśród rozwiązań, które zostały zrealizowane można wymienić np.: aukcje internetowe, sklepy internetowe, serwisy ogłoszeniowe, wirtualne giełdy. Opis konkretnych rozwiązań formowych z tej dziedziny można znaleźć np. w [4].

Rozwój istniejących już gałęzi elektronicznego handlu jak i tworzenie nowych w dużej mierze zależy od popularności Internetu. Prognozy przeprowadzane przez wiele firm badawczych jednoznacznie wskazują na ciągły wzrost użytkowników Internetu na świecie. Bania przeprowadzone przez TNS OBOP, wskazują, że pod koniec 2003 roku dostęp do Internetu deklarowało 29% powyżej 15 roku życia, z czego 23% korzysta z niego przynajmniej raz w miesiącu.

Innym istotnym sygnałem wskazującym na znaczne rozprzestrzenianie się Internetu w Polsce są wyniki przedstawione przez Telekomunikację Polską. Usługa „Neostarada", uruchomiona przez TP, w maju 2004 roku osiągnęła dwieście tysięcy użytkowników, a prognozy wskazują, że na początku 2005 roku liczba ta ma się podwoić.

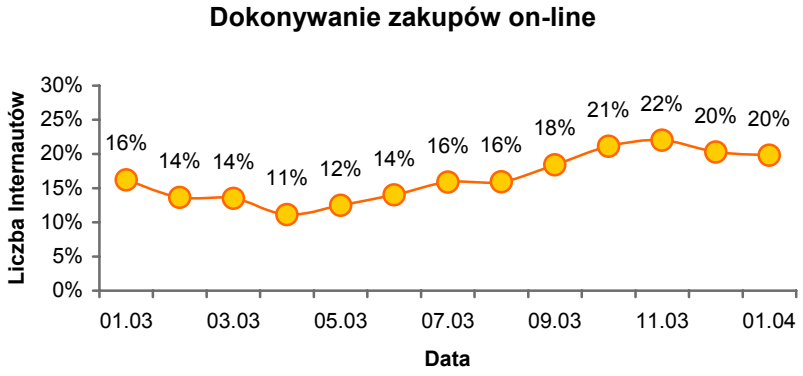

Tabela 1. Dokonywanie zakupów on-line. Źródło: TNS OBOP.

Istotnym badaniem dla e–commerce jest jaki procent Internautów dokonuje zakupów przez Internet. Firma badawcza TNS OBOP, wskazuję, że w listopadzie 2003 roku wyniósł on rekordowo o 22% (tabela 1).

Przedstawione prognozy są bardzo optymistyczne, nie mniej jednak istnieje wiele trudności, które powstrzymują rozwój elektronicznego handlu.

1.3. Bariery dla rozwoju e-commerce.

Charakterystyczną cechą usług e-commerce jest rodzaj informacji biorących w nim udział. Informacja, jako zasób najbardziej pożądany, powinna być w szczególny sposób chroniona. Współczesne technologie pozwalają zadbać o odpowiedni poziom bezpieczeństwa przesyłanych danych, głównie wykorzystując mechanizmy kryptograficzne. Możemy zadbać: o *integralność danych* (informacje zostaną wymienione bez jakichkolwiek poprawek czy zmian), o *poufność danych* (informacje zostaną przekazane w sposób tajny, możliwość ich odczytani będą miały tylko upoważnione osoby), o *anonimowość danych* (informacje mogą być przesyłane w sposób, który nie będzie ujawniał tożsamości nadawcy, odbiorcy), oraz niezaprzeczalności danych (informacja wysłana lub odebrana przez nadawcę/odbiorcę jednoznacznie wskazują na ten fakt bez możliwości oszukania).

Pomimo zapewnień organizacji zajmujących się elektronicznym handlem o bezpieczeństwie zakupów, właśnie bezpieczeństwo jest jedną z głównych barier w rozwoju e-commerce (tabela 2) [5]. Badania wskazują, że 69% ankietowanych podało

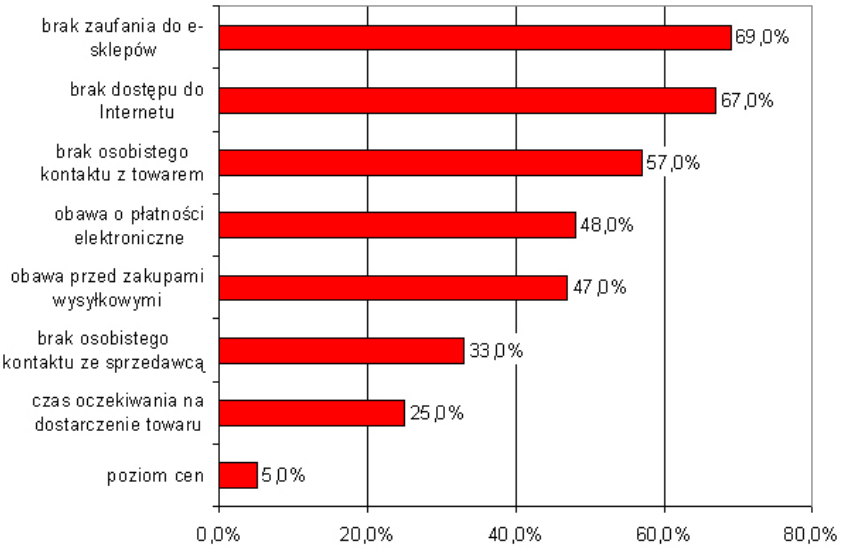

Tabela 2. Powody, dla których konsumencie nie dokonują zakupów przez Internet.

„brak zaufania do e-sklepów” jako główną przyczynę powstrzymywania się od dokonywania zakupów przez Internet. Kolejnym elementem wpływającym na ogólną ocenę bezpieczeństwa jest „dokonywanie płatności w sposób elektroniczny”; blisko połowa ankietowanych wyraziło tą obawę.

Innym czynnikiem, który hamuje rozwój handlu elektronicznego w Polsce jest słaba infrastruktura telekomunikacyjna. 67% ankietowanych nie posiada dostępu do Internetu. W dużych miastach blisko połowa mieszkańców może skorzystać z Internetu natomiast jedynie 16% mieszkańców wsi posiada taką możliwość (tabela 3).

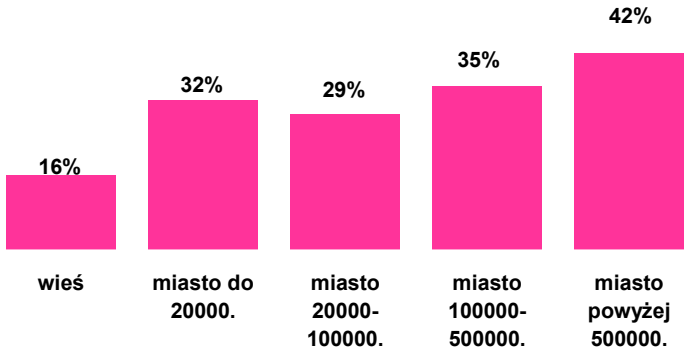

Tabela 3. Dostęp do Internetu w zależności od miejsca zamieszkania. Źródło: TNS OBOP.

Firmy inwestujące w e-commerce powinny posiadać dostęp do szerokopasmowych łączy Internetowych. W wielu małych miasteczkach oraz wsiach Polski nie ma przyłączy do szybkich sieci Internetowych. W dużych miastach Polski dostęp do szerokopasmowych łącz Internetowych jest na poziomie europejskim, niestety opłaty są kilkakrotnie większe niż w Europie.

2. Zagrożenia

Analizując zagrożenia istniejącego handlu elektronicznego oraz jego rozwoju, bezpieczeństwo informacji wydaje się być kluczowym zagadnieniem. Aktualnie w procesie e-commerce główną rolę pełnią aplikacje typu klient-serwer; przykładem mogą być aplikacje bazujące na WWW. Bezpieczeństwo takich usług sieciowych ma trzy newralgiczne elementy. Składają się na nie [6]:

- Bezpieczeństwo po stronie klienta;
- Bezpieczeństwo wymiany danych;
- Bezpieczeństwo po stronie serwera.

Szczegółowa analiza wspomnianych zagadnień jest bardzo złożona. Zajmuje się nimi wiele organizacji tworząc odpowiednie normy, które wyznaczają praktyczne standardy bezpieczeństwa, np. [7], [8], [9], [10], por. też [11]. W pracy tej zwrócimy uwagę na niektóre zagadnienia związane z zapewnieniem bezpieczeństwa, zwłaszcza takie, które można stosunkowo łatwo wprowadzić w systemie e-commerce.

2.1 Klient

Strona klienta opisuje zabezpieczenia po stronie użytkownika systemów e-commerce. Istotnym elementem jest prawidłowe zabezpieczenie systemów operacyjnych oraz aplikacji, z których klienci elektronicznego handlu korzystają. W

tym celu należy zadbać między innymi o najnowsze uaktualnienia systemów, aplikacji oraz baz wirusów programu antywirusowego. Warto również zaopatrzyć się w osobistą „ścianę ognia", która pomoże uchronić komputery klienckie przed niepożądanym ruchem z sieci. Zazwyczaj mniejszą rolę przywiązuje się do komputerów klienta niż serwera, powoduje to, że są one celem wielu ataków.

2.2 Wymiana danych

Ochrona informacji przekazywanych między klientem a serwerem jest kolejnym istotnym składnikiem bezpieczeństwa. Informacje przekazywane przez Internet są narażone na wiele zagrożeń [12]. Są one związane z ich poufnością, anonimowością, niezaprzeczalnością, integralnością. Korzystając z aplikacji, które posiadają zaimplementowane moduły kryptograficzne można zapewnić stosowny poziom bezpieczeństwa. Głównie używane moduły kryptograficzne to: podpis cyfrowy, szyfrowanie, schemat podziały sekretu i inne protokoły kryptograficzne a także funkcje kryptograficzne.

2.3 Serwer

Ochrona danych zgromadzonych na serwerze oraz zabezpieczenie samego serwera, to kolejne elementy bezpieczeństwa. Serwer, jako komputer dzielący określone usługi, posiadający dostęp do wielu informacji, jest ogniwem mocno zagrożonym. Bezpieczeństwo serwerów sieciowych powinno stać na najwyższym poziomie, zagadnienie to jest bardzo obszerne i zróżnicowane. Chcąc sprostać wymaganiom należy pamiętać o wprowadzonych normach dotyczących bezpieczeństwa [7] i stworzyć własne mechanizmy zapewniające stosowny poziom bezpieczeństwa.

3. Krytyczne niebezpieczeństwa

Ataki na infrastruktury teleinformatyczne posiadają różny charakter oraz różne natężenie [13] (tabela 4). Najbardziej powszechnym nadużyciem, jest „gromadzenie

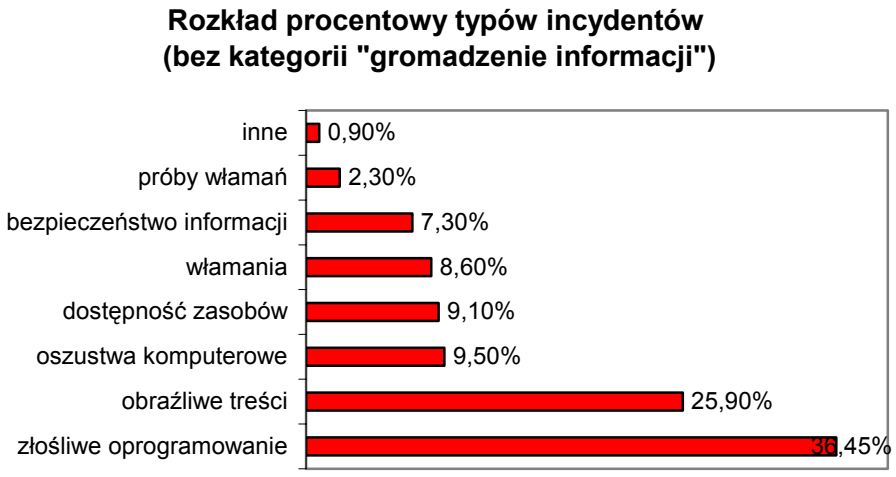

Tabela 4. Rozkład procentowy typów incydentów.

informacji", czyli głównie *skanowanie*. Według CERTU Polska, liczba tego typu incydentów nie przedstawia realnego zagrożenia dla infrastruktury sieciowej ponieważ nie świadczy to wyłącznie o przygotowywaniu przyszłych, ataków ale jest następstwem wcześniej udanych ataków na sieci i komputery.

Główne typy odnotowanych incydentów przedstawione w tabeli 4, pokazują różnorodność możliwych nadużyć w Internecie. Incydenty towarzyszące procesom, które realizują usługi e-commerce, można podzielić na dwie grupy: incydenty zagrażające klientom oraz incydenty zagrażające podmiotom świadczącym usługi (serwerom). Analizując bezpieczeństwo usługi e-commerce jako pewnego procesu, warto zauważyć, że krytyczne niebezpieczeństwo procesu leży w dużym stopniu po stronie serwera usług, a w mniejszym po stronie klienta.

3.1. Klient usług e-commerce

Zanotowane nadużycia przez CERT Polska w roku 2003 [13], wskazują, że najpowszechniejszym zagrożeniem poprawności użycia usług e-commerce, jest „złośliwe oprogramowanie". W jego skład wchodzą głównie robaki sieciowe, wirusy oraz konie trojańskie. Innymi, powszechnie stosowanymi nadużyciami są „niechciane lub obraźliwe treści", czyli spam. Wspomniane ataki nie stanowią jednak dużego zagrożenia dla procesu e-commerce ponieważ ich szkodliwość dla klienta jest dosyć niska, a zapobieganie stosunkowo proste.

Oprócz incydentów mało szkodliwych, można zauważyć nadużycia bardzo groźne. W ich skład wchodzą „włamania" (włamania na konto uprzywilejowane lub zwykłe), „oszustwa komputerowe" (nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszycie się), „bezpieczeństwo informacji" (nieuprawniony dostęp do informacji). Przykładem ilustrującym potencjalne zagrożenie dla procesów e-commerce może być atak składający się z wymienionych incydentów. Pierwszym krokiem może być zdobycie uprawnień uprzywilejowanych („włamanie") w pewnym systemie operacyjnym komputera klienckiego. Drugi krok może polegać na nieuprzywilejowanym dostępie do informacji („bezpieczeństwo informacji"). Ostatecznym krokiem może być podszycie („oszustwo komputerowe"), z pomocą którego można zdalnie wysłać poufne informacje zdobyte w kroku drugim jako całkiem inna osoba na przykład ofertę w aukcji internetowej której realizacja doprowadza do bankructwa .Powszechność takiego rodzaju ataków jest stosunkowa niska nie mniej jednak konsekwencje mogą być bardzo wysokie.

3.2. Serwer usług e-commerce

Serwer usług e-commerce jest elementem krytycznym całego procesu. Głównym powodem takiego stwierdzenia jest fakt, że większość usług e-commerce nie może być poprawnie zrealizowana bez pośrednictwa różnych serwerów sieciowych. Nadużyciami, które wydają się być zagrożeniem dla serwerów sieciowych mogą być „włamania", „oszustwa komputerowe", „bezpieczeństwo informacji" oraz „dostępność zasobów" (ataki blokujące DoS oraz DDoS). Wymienione ataki mają miejsce z podobną częstotliwością, zagrożenia są podobne jak w przypadku opisywanym dla klienta z tą różnicą, że informacje przechowywane na serwerach są zazwyczaj krytyczne.

Wśród wspomnianych incydentów warto wyróżnić jeden, czyli „dostępność zasobów". Ataki te polegają na blokowaniu serwerów (np. rozproszony atak odmowy usługi, DDoS), ich szczególne niebezpieczeństwo tkwi w tym, że ich powstrzymanie

jest szczególnie trudne, a czasami praktycznie niemożliwe do wykonania. W tym wypadku nadużycia niegroźne dla pojedynczego klienta (np. bombardowanie spamem), może doprowadzić do dużych strat dla dostawcy usługi e-commerce powstałych w wyniku uniemożliwienia pracy serwera.

4. Bieżące rozwiązania bezpieczeństwa

Ochrona infrastruktury teleinformatycznej danej organizacji jest zagadnieniem bardzo złożonym. Konkretne wdrażane rozwiązania powinny być poprzedzone stworzeniem polityki bezpieczeństwa, w obrębie której nie zawierają się konkretne rozwiązania a ogólne wymogi. Dzięki ogólnemu charakterowi polityki można ją zastosować w dowolnym momencie rozwoju technologicznego ponieważ zmieniając konkretne rozwiązania informatyczne nie naruszamy zdefiniowanej polityki bezpieczeństwa. Analizując ataki przeprowadzane w 2003 roku zarejestrowane przez CERT Polska, można wskazać obszary zabezpieczeń, które są niezbędne dla bezpiecznego systemu teleinformatycznego.

4.1. Klient usług e-commerce

W skład najliczniejszych ataków na systemy operacyjne klientów usług e-commerce wchodzą robaki sieciowe, wirusy, trojany oraz spam. Robaki sieciowe, wirusy oraz trojany mają różny charakter, mogą być niegroźne, które jedynie rozprzestrzeniają się w sieci komputerowej (np.: „Korgo.I") oraz takie, które blokują duże serwisy Internetowe (atak DDoS: np.: „Kozog"). Zagrożenie może być duże ale przeciwdziałanie jest dosyć proste ponieważ, wystarczy posiadać odpowiednią ochronę antywirusową z aktualnymi bazami sygnatur wirusów żeby prawdopodobieństwo skutecznej infekcji zmalało znacznie. Raporty mówiące o bezpieczeństwie w Internecie [14] wskazują, że o poprawną ochronę antywirusową dba około 76% użytkowników.

Wirusy oraz robaki Internetowe nie są silną bronią ponieważ, rzadko wymierzone są w konkretną organizację, a raczej rozprzestrzeniane są masowo licząc na błędy w systemach operacyjnych oraz aplikacjach komputerowych.

Innymi masowo używanymi nadużyciami są „nie oczekiwane przez odbiorcę treści", czyli najczęściej spam. Szkodliwość tego typu ataku jest mała ponieważ zasadniczo nie powodują one zniszczeń w systemach komputerowych, a jedynie powodują dodatkową pracę przy filtrowaniu otrzymywanych wiadomości. Istnieją aplikacje, które mogą zająć się filtrowaniem aplikacji za nas, badania wskazują [14], że około 20% użytkowników Internetu, korzysta z ich pomocy.

Oprócz wspomnianych ataków sieciowych, istnieją inne, które mogą być bardzo groźne. Są to: „włamania", „oszustwa komputerowe", ataki naruszające „bezpieczeństwo informacji". Komputery klientów usług e-commerce są zazwyczaj w dużo mniejszym stopniu zabezpieczone niż serwery, dlatego skuteczność wspomnianych ataków wobec klientów jest duża. Powodem takiego stanu rzeczy jest zazwyczaj fakt, że ewentualne ryzyko wiążące się z udanym atakiem na taki system, jest małe w porównaniu z kosztem skutecznych zabezpieczeń. Podstawową ochroną przed włamaniami są systemy zapory sieciowej (firewall, ściana ogniowa), czyli oprogramowania służącego do pełnej kontroli ruchu w komputerze klienta, wchodzącego i wychodzącego. Badania pokazują [13], że ponad 50% użytkowników Internetu korzysta z takiej ochrony. Należy również pamiętać o poprawkach wydawanych do używanych systemów oraz aplikacji komputerowych, gdyż w głównej mierze za pomocą luk w oprogramowaniu możliwe są wspominane nadużycia.

Odpowiedzią na ataki związane z bezpieczeństwem informacji oraz oszustwami komputerowymi mogą być systemy ochraniające integralność danych oraz dostęp do danych. W tym celu systemy te najczęściej wykorzystują moduły kryptograficzne. Przykładem mogą systemy szyfrowania plików (chroniące dostęp do informacji przesyłanej i przechowywanej) oraz aplikacje korzystające z podpisu cyfrowego (zapobiegające podszyciu się i innym oszustwom).

Pomimo możliwości technologicznych, komputery klientów usług e-commerce, są w swej większości słabo zabezpieczone. Inaczej jest w przypadku serwerów usług e-commerce.

4.2. Serwer usług e-commerce

Serwery sieciowe są elementami krytycznymi dla całego procesu e-commerce. Wspominane ataki takie jak: „włamania", „oszustwa komputerowe", ataki na „bezpieczeństwo informacji" oraz „dostępność informacji" są najczęstszymi atakami na serwery usług e-commerce. Metody ochrony przed takimi atakami są podobne jak w przypadku klientów z tą różnicą, że o bezpieczeństwo serwerów dba zazwyczaj zespół specjalistów, stale śledzących zagrożenia w Internecie. Implementacja infrastruktury teleinformatycznej jest poparta stosowną polityką bezpieczeństwa, a jej realizacja opiera się na wyznaczonych standardach bezpieczeństwa [7].

Istotnymi elementami zwiększającymi ochronę informacji, zarówno serwerów jak i całego procesu e-commerce są moduły kryptograficzne. Szczególnie silną bronią przed nadużyciami są protokoły kryptograficzne, które korzystając z wielu technologicznych mechanizmów jakie daje np. kryptografia, pozwalają w skuteczny sposób zadbać o ochronę informacji. O sile protokołu stanowią jego właściwości [15]:

- Każdy użytkownik protokołu musi go znać i kolejno wykonywać wszystkie kroki.
- Każdy użytkownik musi zgodzić się na jego stosowanie.
- Protokół nie może mylić; każdy krok powinien być dobrze zdefiniowany i nie może wystąpić jakakolwiek szansa na nieporozumienie.
- Protokół musi być kompletny; dla każdej możliwej sytuacji musi być podany odpowiedni sposób postępowania.
- Protokół powinien zezwalać jedynie na wykonywanie takich operacji, które są w nim przewidziane.

Przykładowymi protokołami kryptograficznymi mogą być: protokół elektronicznego głosowania [16], zaliczany do tzw. elektronicznej demokracji (e-democracy) lub protokół elektronicznego przetargu [17], realizujący jedno z zadań e-commerce. Dzięki protokołom kryptograficznym możemy uzyskać właściwy poziom ochrony informacji, zapewniając między innymi anonimowość źródła danych i ich celu przeznaczenia, integralność, poufność i niezaprzeczalność informacji, a także odpowiednią autoryzacje informacji.

5. Podsumowanie

W pracy zaprezentowano kierunki rozwoju usług e-commerce, możliwości jakie się przed nimi otwierają oraz zagrożenia, które czyhają na tego rodzaju procesy. W ciągu ostatnich kilku lat aktywność firm w sektorze elektronicznej gospodarki znacznie się zwiększa. Proces ten jest jednak zagrożony, istniej wiele barier, które hamują rozwój elektronicznego handlu. Za główną przyczynę blokującą rozwój e-commerce można

uznać bark zaufania inwestorów oraz klientów usług internetowych do gwarantowanego w tych usługach poziomu bezpieczeństwa informacji. Innym, ważny elementem jest słabo rozwinięta infrastruktura teleinformatyczna kraju, co wiąże się z małą dostępnością omawianych usług.

Problem bezpieczeństwa informacji wykorzystywanych w procesie e-commerce jest złożony. W tej pracy przedstawiono główne zagrożenia na jakie narażone są informacje oraz możliwe sposoby ich ochrony.

Literatura:

1. B. Gregor, M. Stawiszyński; "e-Commerce"; Oficyna Wydawnicza Branta; 2002.
2. Sewilla European Council; "An information society for all – Commission of the european communities"; eEurope 2005; 21/22 June 2002.
3. Ministerstwo Nauki i Informatyzacji; „Strategia Informatyzacji Rzeczypospolitej Polskiej - ePolska"; maj 2003.
4. T.R.Köhler, R.B.Best; "Electronic Commerce. Koncepcje, realizacje i wykorzystanie w przedsiębiorstwie", Adison-Wesley i CeDeWu, Warszawa 2000.
5. A. Kaniewska-Sęba, G. Leszczyński; „Postrzeganie e-commerce w polskich sklepach detalicznych – wyniki badań"; Świat Marketingu; październik 2003.
6. J.Francik, K.Trybicka-Francik;„Gospodarka elektroniczna – perspektywy i bariery"; Studia Informatica v. 22; 2001.
7. ISO/IEC; "Information technology – Code of practice for information security management"; ISO/IEC 17799; 2002.
8. W3C Recommendation: XML Encryption Syntax and Processing, http://www.w3.org/TR/XMLENC-CORE.
9. W3C Recommendation: XML Signature Syntax and Processing, http://www.w3.org/TR/XMLDSIG-CORE.
10. Security in a Web Services World: A Proposed Architecture and Roadmap, http://www-106.ibm.com/developerworks/webservices/library/ws-secmap.
11. W.Karwowski, A.Orłowski; Bezpieczeństwo usług WWW, Materiały VIII Krajowej Konferencji Zastosowań Kryptografii Enigma 2004, K-321-330.
12. CERT Polska; "Zabezpieczenie prywatności w usługach internetowych"; CERT Polska;2001r.
13. CERT Polska; „Analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003"; CERT Polska; 2003.
14. G. Gros; „Bezpieczeństwo w Internecie, Polska 2004 r."; Symantec Polska; 2004 r.
15. B. Schneier; „Kryptografia dla praktyków"; Wydawnictwo Naukowo-Techniczne, Warszawa; 2002.
16. L. Barlow; „A Discussion of Cryptographic Protocols for Electronic Voting"; 2003 r.
17. B. Księżopolski, Z. Kotulski; "Cryptographic protocol for electronic auctions with extended requirements"; Annales UMCS Informatica; 2004.