Biuro Generalnego Inspektora
Ochrony Danych Osobowych,
Pl. Powstańców Warszawy 1
00-030 Warszawa

PROBLEMY OCHRONY DANYCH OSOBOWYCH WE WSPÓŁCZESNYCH, ROZPROSZONYCH SYSTEMACH TELEINFORMATYCZNYCH

Andrzej Kaczmarek

Wstęp.

Mówiąc o danych osobowych mamy najczęściej na myśli dane określające tożsamość osoby, jej miejsce zamieszkania, poziom wykształcenia, doświadczenie zawodowe, itp. Dane te znane są najczęściej w otaczającym nas środowisku. Służą one celom komunikowania i porozumiewania się. Najczęściej nie zależy nam na tym, aby dane tego typu chronić w jakiś szczególny sposób. Wręcz przeciwnie, zainteresowani jesteśmy raczej tym, aby w najbliższym nam otoczeniu dane te były znane. O tym jednak, jakie informacje o sobie i komu mamy ochotę przekazać, chcemy decydować sami. Nie jesteśmy obojętni na rozpowszechnianie o nas informacji w środowiskach nam nieżyczliwych, mało znanych lub nieznanych w ogóle. Potrzeby ochrony naszych danych nasilają się szczególnie wówczas, gdy mogą one być wykorzystane na naszą szkodę. Najczęściej nie chodzi wtedy tylko o podstawowe dane osobowe takie jak imię, nazwisko i adres, ale również o inne, dodatkowe dane dotyczące np. cech charakteru, stanu majątkowego, stanu zdrowia, życia rodzinnego itp. Dane takie, nazywane często danymi osobistymi lub po prostu prywatnością, staramy się chronić w szczególny sposób. Ochrony takich danych mamy prawo wymagać również od innych - patrz [1,2,3,4,5].

Potrzeba prawnej ochrony danych osobowych wynika głównie stąd, iż niezależnie od naszej woli, informacje nas dotyczące mogą pozyskiwać osoby, które nie zawsze potrafią zachować ją wyłącznie dla siebie. Niektórzy w posiadanie takich informacji wchodzą z racji wykonywania określonego zawodu. Problem ten istnieje od dawna i w celu jego uregulowania wypracowano wiele regulaminów i norm prawnych określających zasady postępowania tych, którzy w posiadanie określonych kategorii informacji osobowych wchodzą w wyniku świadczenia usług jak np. lekarze, psycholodzy, prawnicy, itp. lub w wyniku wykonywania prawnie uzasadnionych obowiązków rejestracyjnych, co dotyczy np. pracowników niektórych instytucji i urzędów.

Do niedawna informacje, o których mowa wyżej przechowywane były głównie w pamięci osób, które je pozyskały, w sporządzanych przez nie notatkach, dokumentach lub księgach rejestrowych. Dostęp do tak przechowywanych informacji był wyraźnie ograniczony. Z jednej strony były to, jak już wspomniano formalne ograniczenia natury prawnej, z drugiej zaś rzeczywiste ograniczenia natury technologicznej. Te ostatnie były w przeszłości głównym czynnikiem, który w naturalny sposób ograniczał skalę nielegalnego przetwarzania danych osobowych. Nie jest bowiem łatwo wbrew woli człowieka wykraść zapamiętaną przez niego informację. Pozyskanie zaś informacji zawartej w notatkach, czy rejestrach wymaga dużego nakładu pracy i bezpośredniej ich dostępności.

Przedstawioną sytuację w zasadniczy sposób zmieniła technologia cyfrowego kodowania informacji zastosowana w praktyce po raz pierwszy w latach 80-tych XIX wieku do przetwarzania danych demograficznych w powszechnych spisach ludności Stanów Zjednoczonych Ameryki Północnej przez Hermann H. Holleritha. Technologia ta sprawiła, że dane osobowe zebrane podczas spisu w 1900 r. na 63 mln specjalnie przygotowanych kartach przetworzono w niespełna jeden miesiąc, uzyskując szczegółowe dane demograficzne. Prawdziwy boom w automatycznym przetwarzaniu informacji nastąpił jednak dopiero w drugiej połowie ubiegłego stulecia, kiedy to technologia przetwarzania cyfrowego

wsparta osiągnięciami w dziedzinie technologii elektronicznej znalazła szerokie zastosowanie w rodzącym się przemyśle komputerowym, a następnie również w telewizji i telekomunikacji. Niemały wpływ na rozwój technologii cyfrowego przetwarzania informacji miały również technologie zapisu informacji cyfrowej umożliwiające jej gromadzenie i przechowywanie w niespotykanych dotąd ilościach.

Wymienione czynniki spowodowały powstanie nowych kategorii informacji w sieciach komputerowych i telekomunikacyjnych. Obecnie operator usług telekomunikacyjnych może przetwarzać nie tylko informacje o treści przesyłanych dokumentów bądź rozmów, ale również informacje o tym, do kogo przesyłamy dokument, z kim rozmawiamy, kiedy i jak długo. Rozwój technologii komputerowej w kierunku sieci komputerowych i tzw. rozproszonego przetwarzania spowodował, że przetwarzanie informacji wyszło poza ściśle określone środowiska centrów obliczeniowych. Do jej przesyłu wykorzystano istniejące łącza sieci telefonicznych, jak również specjalne linie światłowodowe o ogromnych możliwościach transmisji zwane infostradami informacyjnymi. Coraz częściej do transmisji danych cyfrowych wykorzystuje się również środki łączności bezprzewodowej. Mający dostęp do takich sieci operator usług telekomunikacyjnych może wejść w posiadanie przesyłanej tam informacji. Jeżeli informacja ta nie jest kodowana, może się z niej dowiedzieć o usługach Internetowych, z których korzystamy, o adresach komputerów, z którymi się łączymy, adresach odwiedzanych stron WWW, odbiorcach prowadzonej korespondencji, a w niektórych przypadkach nawet o jej treści. Sama technologia informatyczna, pomimo że teoretycznie umożliwia stworzenie odpowiednich mechanizmów autoryzowania, kontroli i poufnej dystrybucji przetwarzanej informacji, to w praktyce nie zawsze nadąża za zmianami i modyfikacjami stosowanych w tym celu narzędzi. Ponadto ich praktyczne stosowanie nie zawsze jest przyjazne dla przeciętnego użytkownika, a w niektórych przypadkach nawet dla profesjonalistów. Czynniki te w konsekwencji stwarzają poważne zagrożenia dla poufności przetwarzanej informacji.

1. Zagrożenia ochrony danych osobowych w systemach informatycznych.

Jak już wspomniano nowy wymiar problemów dotyczących ochrony danych osobowych niewątpliwie związany jest z technologią teleinformatyczną. Przyczyn jest wiele, najważniejsze jednak to szybki rozwój technologii teleinformatycznych i niemal natychmiastowe ich wdrażanie bez wystarczającej analizy jakości używanych narzędzi i środowiska teleinformatycznego, w którym zostają zastosowane. Technologie te wdrażane są najczęściej w czasie, kiedy brak jest jeszcze standardów w zakresie bezpiecznego ich stosowania. Te pojawiają się bowiem dopiero po określonym czasie doświadczeń i obserwacji, co jest niezbędne dla ich weryfikacji. Dziś po kilkuletnich doświadczeniach posiadamy np. określone standardy i metody dotyczące projektowania i eksploatacji zwłaszcza lokalnych, scentralizowanych systemów baz danych. Wypracowane i sprawdzone zostały w praktyce określone technologie i metody dotyczące projektowania, zarządzania i ochrony określonej kategorii systemów informatycznych. Organizacje normalizacyjne wypracowały w tym zakresie odpowiednie standardy i klasyfikacje [7,8,9], które wykorzystywane są nie tylko dla celów projektowych, ale również w celu opracowania różnego rodzaju regulaminów i aktów prawnych. Tak np. w rozporządzeniu dotyczącym podstawowych warunków jakim powinny odpowiadać systemy informatyczne służące do przetwarzania danych osobowych [6] wykorzystuje się wypracowane standardy potwierdzania tożsamości operatora systemu informatycznego. Wymienia się tam miedzy innymi, iż dostęp do przetwarzania danych powinien być możliwy po wprowadzeniu *identyfikatora użytkownika* i *hasła*. Podobnie wykorzystuje się określone standardy przetwarzania danych w systemach informatycznych do wskazania wymogów w zakresie dokumentowania określonych zdarzeń.

Wspomniane standardy nie wystarczają jednak do rozwiązywania bieżących problemów dnia dzisiejszego związanych ze stosowaniem najnowszych osiągnięć technologii elektronicznej i inżynierii oprogramowania. Dziś, jak już wspomniano, dane osobowe nie tylko są przetwarzane w scentralizowanych systemach informatycznych, ale przede wszystkim w rozproszonych środowiskach

sieciowych, gdzie fizyczna lokalizacja danych może być oddalona od źródła ich pozyskiwania czy też udostępniania o setki a nawet tysiące kilometrów. Sam schemat przetwarzania zaś został tak rozproszony i zautomatyzowany, że użytkownik stracił praktycznie kontrolę nad tym w jaki sposób i z wykorzystaniem jakich łączy i mediów dane te są przesyłane. Decyzje w tym zakresie podejmowane są automatycznie przez specjalistyczne urządzenia optymalizujące i nadzorujące przepływ informacji [10,11]. Technologie Internetu oraz cyfrowej telefonii komórkowej, zrewolucjonizowały przetwarzanie danych i to nie tylko pod względem technologicznym, ale również organizacyjnym.

Coraz częściej przez Internet zamawiamy różne usługi i towary. Przez Internet przesyłamy dyspozycje do banku, czy też maklera giełdowego. Za pośrednictwem Internetu organizujemy wolny czas, rezerwujemy bilety w kinach, teatrach i operach. Przez Internet rezerwujemy hotel i bilety lotnicze. Jak wynika z ostatnich doniesień prasowych, przez Internet lub telefon komórkowy będziemy mogli wnosić opłaty za korzystanie z parkingu, w tym również przedłużyć okres deklarowanego czasu parkowania. Wiele mówi się o projektach użycia telefonu komórkowego do realizacji płatności za korzystanie ze środków komunikacji miejskiej i innych, drobnych świadczeń. Obserwujemy integrację usług dostępnych w sieciach komputerowych z usługami telefonii cyfrowej. Internet poprzez rozwój łączności bezprzewodowej staje się coraz bardziej mobilny. Do integracji Internetu i telefonii komórkowej stworzono specjalne protokoły przesyłania informacji takie jak GPRS oraz WAP bazujące na protokole pakietowej transmisji danych IP. Integracja ta przynosi nam często wymierne korzyści, których przykładem jest wykorzystanie pakietowej transmisji danych do realizacji usług typowo telefonicznych VoIP (Voice over IP) oraz pakietowej transmisji danych w bezprzewodowych sieciach telefonicznych (protokół GPRS).

2. **Dane osobowe i internet.**

Mówiąc o ochronie danych osobowych w Internecie i w ogóle we współczesnych systemach teleinformatycznych należy mieć na uwadze przede wszystkim bezpieczeństwo danych zapisanych w urządzeniach podłączonych fizycznie do węzłów sieci teleinformatycznych, które włączone są w strukturę Internetu oraz bezpieczeństwo danych, które łączami tymi są przekazywane. W pierwszym przypadku rozwiązanie problemu polega na skonstruowaniu odpowiednich mechanizmów autoryzacji i zastosowaniu specjalnych narzędzi zwanych ścianami ogniowymi (firewall). Ich zadaniem jest ochrona danego systemu lub sieci lokalnej przed nieautoryzowanym dostępem do danych lub ich zniszczeniem. W drugim przypadku, problem sprowadza się głównie do zabezpieczenia danych w fazie ich transportu. Rozwijając nieco głębiej ten ostatni temat, należy wyjaśnić, iż technologia przesyłu informacji, którą wykorzystuje Internet zwana popularnie protokołem TCP/IP powstała w latach 70 tych dla potrzeb wojskowych. Planowana do wykorzystania w zamkniętych strukturach nie zawierała specjalnych rozwiązań umożliwiających ochronę przesyłanych danych przed nieautoryzowanym podglądem. Przekazana pod koniec lat 80-tych do użytku cywilnego, głównie dużych korporacji i środowiska akademickiego wykorzystywana była do wymiany informacji w badaniach naukowych oraz ich organizacji. Były to zastosowania, które nie wymagały specjalnych zabezpieczeń.

Problem ochrony i bezpieczeństwa informacji nasilił się dopiero w latach 90 tych kiedy to powstał protokół WWW i Internet zaczął trafiać do coraz szerszego kręgu odbiorców. Stało się to głównie za sprawą zarówno rozwoju technologii elektronicznej jak i technologii oprogramowania, dzięki której korzystanie z różnych usług internetowych stawało się coraz łatwiejsze. W wyniku tych przeobrażeń zmieniła się społeczność internetowa. Sam Robert Cailliau - jeden z współtwórców popularnego dziś WWW powiedział: "Niegdyś społeczność internetowa była jednorodna i cywilizowana. Dziś tak nie jest, Internet stał się chaosem, a my jesteśmy w jego środku". Czy rzeczywiście tak jest? Odpowiedź jest twierdząca. Dziś Internet stał się potężnym narzędziem reklamy. Powstały sklepy internetowe, które umożliwiły robienie zakupów bez wychodzenia z domu. Dla wielu Internet stał się narzędziem pracy, dla innych narzędziem rozrywki. Dzięki Internetowi stało się możliwe szybkie gromadzenia różnorodnych

danych, w tym również danych osobowych. Dane te mogą być pozyskiwane za pośrednictwem różnych usług, w tym stron internetowych WWW, poczty elektronicznej, grup dyskusyjnych czy też pogawędek zwanych Chatami lub IRCami od angielskiej nazwy Internet Relay Chat (IRC).

Korzystanie z większości wymienionych usług jak również ich świadczenie nie jest w sieci Internet dla nikogo ograniczane. Usługę poczty elektronicznej, czy też dystrybucji własnej strony WWW wielu operatorów oferuje nieodpłatnie w celu poszerzenia kręgu osób, którym mogą przekazywać informacje reklamowe. To stwarza sytuację, w której niezidentyfikowany z uwagi na brak jakichkolwiek formalnych powiązań z administratorem użytkownik może aktywnie zaistnieć w Internecie. Może on tym samym utworzyć własną stronę WWW i za jej pośrednictwem przetwarzać np. dane osobowe. Cechą charakterystyczną wymienionych usług jest to, że zakres ich terytorialnego działanie nie jest technicznie ograniczony. Operator, udostępniający swoje zasoby techniczne i programowe może mieć siedzibę w innym kraju niż użytkownik z nich korzystający. W konsekwencji prowadzi to do trudności w egzekucji określonych czynów jak na przykład zaniechania nielegalnego przetwarzania danych osobowych, nawoływania do przestępstwa, publikowanie obraźliwych tekstów itp.

Niestety, dla niektórych Internet stał się również narzędziem przestępstwa. Używany przez cybernetycznych przestępców może stać się źródłem inspiracji napadów a nawet mordów. "Dane dotyczące kart kredytowych giną w niewyjaśnionych okolicznościach, wirusy szerzą chaos, tajemnice firmowe są ujawniane a handlarze narkotyków sprzedają swój trefny towar" - to obraz przedstawiony w net.komentator [12], gdzie autorzy podają przykłady kilku ujawnionych przestępstw.

Przeglądanie stron WWW

Innym niebezpieczeństwem na jakie narażeni są użytkownicy Internetu jest śledzenie ich zainteresowań poprzez analizę zawartości informacyjnej ich prywatnych komputerów bądź obserwację i analizę ich poczynań w Internecie. W pierwszym przypadku wykorzystuje się fakt, że podczas połączenia z Internetem komputer użytkownika może być obiektem analizy hakerów. Korzystając ze specjalnych narzędzi mogą oni przeszukiwać aktualnie włączone w sieci komputery w poszukiwaniu celów swojego ataku. Celami takimi będą np. komputery, którym wcześniej przesłano specjalne programy typu "backdoors" (tylne wejścia) jak np. Back Orifice, NetBus czy SubSeven, które udostępniają atakującemu zasoby atakowanego komputera. Wśród zasobów tych mogą być teksty, grafika, muzyka, programy oraz zbiory danych, w tym również dane osobowe właściciela komputera zapisane zazwyczaj podczas instalacji licencji na użytkowane oprogramowanie lub konfiguracji niektórych programów np. obsługujących pocztę elektroniczną. Celem ataku hakerów mogą być również komputery, na których zlokalizowano oprogramowanie posiadające luki w zabezpieczeniach systemu operacyjnego lub zainstalowanych na nim programach użytkowych takich jak przeglądarki internetowe - Internet Explorera i Netscape Navigatora czy też programy do wspomagania obsługi biurowej [16]. W wielu przypadkach, aby wykorzystać lukę w zabezpieczeniu zachęca się ofiarę na swoją stronę WWW, po czym bez jego wiedzy przesyła się na jego komputer specjalne polecenia np. skrypty języka JavaScript, które (dzięki lukom) otworzą atakującemu drogę do penetrowania zasobów zaatakowanego komputera.

W drugim przypadku, to jest w czasie przeglądania stron WWW użytkownicy narażeni mogą być, poza opisanymi już przypadkami na śledzenie ich poczynań poprzez odnotowy-wanie adresów stron, które odwiedzają. Działalność taką na szeroką skalę na początku ubiegłego roku prowadziły dwie znane firmy - DoubleClick i Aureate Media Corporation [13]. Pierwsza wykorzystywała w tym celu małe pliki tekstowe, które wysyłają witryny internetowe do odwiedzających je przeglądarek. Podobnie postępuje wiele innych firm internetowych jednak DoubleClick postanowiła spersonalizować uzyskane tą drogą informacje poprzez powiązanie ich z nazwiskami i adresami osób (użytkowników) uzyskanymi z wypełnionych online ankiet. Firma Aureate Media Corporation zaproponowała natomiast internautom narzędzia, które po zainstalowaniu, oprócz swoich użytkowych funkcji okazały się doskonałymi

narzędziami szpiegowskimi [15]. Przesyłały one do firmy Aureate dane o użytkownikach komputerów, ich kontach internetowych oraz wszelkim zainstalowanym w komputerze oprogramowaniu. Najbardziej niepokojącym był jednak fakt, że opisane funkcje szpiegowskie oprogramowania pozostawały na komputerze użytkownika nawet po jego odinstalowaniu.

Dane o zainteresowaniach muzycznych użytkowników swojego sprzętu zbierała także firma Real Networks. W produkowanych przez siebie odtwarzaczach Jukebox zbierała a następnie wysyłała do swojego serwera tytuły odtwarzanych przy ich użyciu plików [13].

Handel elektroniczny.

Jednym z największych źródeł zagrożenia prywatności wydają się być usługi związane z handlem elektronicznym. Dają one duże możliwość monitorowania transakcji w sieci, możliwość uzyskiwanie wiadomości o operacjach finansowych, o zwyczajach i decyzjach handlowych, o zwyczajach konsumpcyjnych klientów itp. Patrząc na zjawisko handlu elektronicznego od strony konsumenta, użytkownik nie zawsze zdaje sobie sprawę z potencjalnych zagrożeń, na jakie narażone są jego dane osobowe. Dotyczy to szczególnie sytuacji, kiedy zamawiając towar w sklepie internetowym klient decyduje się na zapłatę karta kredytową przesyłając jej numer i inne niezbędne do wykonania transakcji dane, nie upewniwszy się wcześniej, jak dane te będą chronione podczas transmisji. Handel elektroniczny ma niewątpliwie przyszłość, ale jego podstawą powinny być starannie wypracowane, sprawdzone i niezawodne metody. Dopuszczone zaś do stosowania w handlu i bankowości systemy komputerowe powinny być w szczególny sposób odporne na wszelkiego rodzaju ataki komputerowe. Niedopuszczalne ze względu na bezpieczeństwo jest stosowanie do tego celu rozwiązań wykorzystujących jawne, nie szyfrowane przesyłanie informacji. W rozwiązaniach przeznaczonych do wykonywania transakcji internetowych w sposób szczególny należy zadbać o wiarygodność i bezpieczeństwo przesyłanych danych. Na każdym jej etapie decyzję powinna podejmować właściwa, uprawniona do tego strona. Oznacza to, że np. decyzję do banku o zapłacie dostawcy za zamówiony towar powinien podejmować właściciel konta bankowego kierując wystawioną przez dostawcę towaru elektroniczną fakturę, a nie dostawca na zlecenie klienta, co w chwili obecnej jest dość często stosowana praktyką. Nie wydaje się uzasadnione, aby w wyniku przeprowadzonej transakcji dostawca wchodził w posiadanie numeru karty kredytowej zamawiającego, wystarczającym powinno być przekazanie przez wskazany bank odpowiednich środków na jej pokrycie.

Usługi lokalizacyjne telefonii komórkowej.

Duże oczekiwania i perspektywy zapowiadają się przed operatorami telekomunikacyjnymi w zakresie usług lokalizacyjnych (LBS - Local Based Services). Już technologia GSM daje w tym zakresie wielkie możliwości, których przykładem są jedne z pierwszych w tym zakresie komercyjnych usług fińskiego operatora Sonera [14]. Usługa Pointer Guide Sonera umożliwia np. użytkownikowi telefonu wyposażonego w przeglądarkę WAP uzyskać informacje o najważniejszych wydarzeniach, atrakcyjnych imprezach i możliwościach zakwaterowania w okolicy najbliższej obszaru, w którym zastała wywołana. Usługa Pointer Friends natomiast pozwala na określenie miejsca pobytu przyjaciół. W przypadku potrzeby udzielenia pomocy użytkownik może skorzystać z usługi Pointer SOS, która umożliwi zlokalizowanie miejsca jego pobytu i monitorowanie jego zmian.

Nie wiadomo jeszcze do końca, jakie nowości przyniesie w tym zakresie telefonia cyfrowa 3 generacji (UMTS). W jakim jeszcze celu będą one stosowane i do jakiego stopnia ograniczyć mogą ostatnie już obszary naszej prywatności. Czy przeraża nas wizja takiej przyszłości? Większość zapewne odpowie, że tak. Jest to wydaje się ostatnia chwila na dialog i podjęcie zintegrowanego wysiłku na rzecz

ochrony prywatności. Właśnie teraz kiedy technologia telefonii komórkowej zwłaszcza 3 generacji jest młoda, a Internet pozwolił zebrać już pierwsze doświadczenia dotyczące zagrożeń prywatności i metod jej ochrony. Wspierając prawnie ustanowione zasady ochrony danych osobowych i konstytucyjne prawo do zachowania prywatności należy uczynić wszystko, aby maksymalnie oddalić wizję urzeczywistnienia się scenariusza naszkicowanego w satyryczno-groteskowej powieści Georga Orwella Rok 1984. W niedługim czasie, może się bowiem okazać, że szpiegowanie naszych działań w Internecie będzie błahostką w porównaniu z tym, co przyniesie technologia bezprzewodowego przesyłu informacji zintegrowana z satelitarnymi usługami lokalizacyjnymi GPS (Global Positioning System).

3. Metody ochrony danych osobowych w rozproszonych systemach teleinformatycznych.

Realizując program ochrony informacji w rozproszonej sieci teleinformatycznej, jaką jest Internet musimy pamiętać, że działania, jakie należy w tym celu wykonać nie tylko będą dotyczyły serwerów, na którym zlokalizowane są duże zbiory danych osobowych, ale również każdego komputera osobistego bądź stacji roboczej, które zostały przyłączone do Internetu. Każdy komputer podłączony do sieci Internet staje się widoczny dla wszystkich innych. Jest on identyfikowany poprzez unikalny adres IP. Nie oznacza to jednak, że widoczne są wszystkie zgromadzone na nim zasoby informacyjne. O tym jak dany komputer będzie widziany w sieci, które ze zgromadzonych na nim danych można zdalnie modyfikować, a które tylko przeglądać może decydować jego główny użytkownik ustawiając odpowiednie zabezpieczenia.

Autoryzacja dostępu

Podstawowym elementem decydującym o dostępności zgromadzonych informacji jest, jak powszechnie wiadomo, nadany im poziom ochrony oraz uprawnienia użytkownika. Celem ochrony może być cały, wydzielony obszar sieci komputerowej, określony komputer, realizowane przez niego usługi lub dostępne mu obszary pamięci masowej. W większości przypadków ochrona ta polega na uwarunkowaniu prawa wykonywania określonych operacji od autoryzacji użytkownika, którą przeprowadza się poprzez porównanie wprowadzonego przez użytkownika hasła z zapamiętanym w systemie wzorcem, poprzez "okazanie" identyfikatora w formie karty magnetycznej lub procesorowej. Coraz częściej stosowane są również tzw. biometryczne metody autoryzacji wykorzystujące obraz linii papilarnych, obraz tęczówki oka, geometrię dłoni, twarzy lub charakterystykę głosu [17]. W systemach rozproszonych i większości zastosowań w aplikacjach Internetowych decydujące znaczenie ma jednak autoryzacja wykorzystująca ideę hasła. Jej skuteczność zależy głównie od trudności przypadkowego odgadnięcia hasła oraz, w skrajnym przypadku, od technicznych możliwości sprawdzenia wszystkich jego kombinacji. Istotna jest tutaj świadomość użytkowników, którzy przecież sami decydują o treści hasła do przyznanych im zasobów informacyjnych i baz danych. Dobrym przykładem ilustrującym ten problem jest wyliczenie przedstawione w dokumentacji programu Office Password, wg którego czas automatycznego sprawdzania wszystkich kombinacji haseł, w którym użyto cały dostępny na klawiaturze zestaw znaków dla komputera z procesorem Pentiunm 200 wynosi odpowiednio: 71 minut dla hasła o długości 4 znaki, 15 miesięcy dla hasła o długości 6 znaków i 11 600 lat dla hasła o długości 8 znaków [18].

Ważnym elementem bezpieczeństwa jest jakość zabezpieczeń i stabilność pracy użytkowanych systemów. Należy jednak pamiętać, że nawet w systemach uznanych za bezpieczne mogą wystąpić błędy. Błędy te, wykryte przez hakerów mogą się okazać bardzo niebezpieczne. Stąd też podstawową regułą administratorów powinno być śledzenie serwisów WWW (np. www.securityfocus.com) i list dyskusyjnych (bugtraq@securityfocus.com) poświęconych bezpieczeństwu oraz regularne instalowanie publikowanych tam poprawek. [19, 20]. W przypadku zdalnego administrowania systemem komputerowym ważnym elementem bezpieczeństwa jest szyfrowanie sesji. Nigdy nie ma bowiem pewności, że biorące udział w transmisji pakietów urządzenia (komputery węzłowe, routery) nie mają zainstalowanego oprogramowania śledzącego (np. snifferów). Urządzenia te pozostają najczęściej poza

kontrolą administratora. W odniesieniu natomiast do konsoli zarządzających, zachować należy wszelkie reguły bezpieczeństwa fizycznego umieszczając je w wydzielonym pomieszczeniu, do którego dostęp mają tylko upoważnione osoby.

Zastosowania szczególnych metody ochrony i środków autoryzacji wymagają również sieci lokalne, w których wykorzystuje się komunikację bezprzewodową. Bezpieczna konfiguracja węzłów takiej sieci wymaga szczegółowej specyfikacji tzw. list dostępowych oraz zdefiniowania bezpiecznej w danym środowisku metody autoryzacji użytkowników. Technologia stosowana do budowy takich sieci jest stosunkowo nowa, zwłaszcza standard IEEE 802.11b, który przełamał szereg ograniczeń w komunikacji bezprzewodowej. Na uwagę zasługuje tutaj fakt, że nie wszystkie jeszcze, używane w tym standardzie do budowy sieci urządzenia umożliwiają zastosowanie zalecanego dla autoryzacji użytkowników standardu RADIUS [30].

Stosowanie usług kryptograficznych

W przypadkach, kiedy celem operacji jest bezpieczne przesłanie danych za pomocą poczty elektronicznej, usługi FTP lub innych narzędzi oraz gdy istota problemy polega na potrzebie ochrony treści przesyłanych informacji przy jednoczesnym zastosowaniu do tego celu środków teletransmisji przewodowej lub bezprzewodowej jedynym skutecznym rozwiązaniem wydają się być narzędzia ochrony kryptograficznej. Ważne jest jednak, aby narzędzia te stosowane były zgodnie z określanymi w ich instrukcjach zasadami. Należy bowiem pamiętać, że szyfrogram będzie bezpieczny jeśli właściwie zabezpieczymy klucz użyty do jego utworzenia.

Do kryptograficznej ochrony danych stosuje się obecnie wiele różnych narzędzi o znanej na ogół metodzie szyfrowania i używanych do ich realizacji algorytmach krypto-graficznych. Głównym wskaźnikiem ich oceny jest odporność zastosowanej metody szyfrowania na kryptoanalizę oraz długość klucza szyfrującego. Do niedawna uważano, że wystarczającym kluczem jest klucz o długości 56 bitów, gdyż do jego brutalnego złamania tj. spróbowania wszystkich jego 10^{16} kombinacji trzeba było wykonać taką liczbę operacji, których wykonanie na komputerze średniej klasy zajęłoby od kilku do kilkuset lat. Szybki rozwój technologii komputerowej oraz możliwości łączenia ich mocy poprzez połączenia w sieci sprawił jednak, że to, co było wystarczające kilka lat temu dziś stało się bezużyteczne.

Za wystarczająco skuteczne uważa się dziś algorytmy szyfrujące wykorzystujące klucze o długości 128 i więcej bitów. Do jego brutalnego złamania, czyli zidentyfikowania użytego klucza poprzez sprawdzenie wszystkich jego kombinacji trzeba sprawdzić 10^{38} takich kluczy, co jak wyliczył Bruce Schnejer [29], dla maszyny o wartości około milion dolarów o mocy przewidywanej dla takiej maszyny na rok 2005 zajmie około 10^{20} lat. Wg wielu opinii za wystarczająco bezpieczny można dziś uznać również odporny na krypto-analizę algorytm 3DES, w którym następuje trzykrotne szyfrowanie wiadomości z użyciem dwóch różnych 64 bitowych kluczy co daje razem klucz o długości 112 bitów.

Do ochrony transmisji danych w sieciach komputerowych można również stosować specjalne protokóły takie jak Secure Shell (SSH) i Secure Socket Layer (SSL). Ten ostatni, opracowany i udostępniony do użytku publicznego przez firmę Netscape, stał się protokołem powszechnie używanym w sieci Internet. W protolole SSL do kodowania przesyłanych informacji wykorzystuje się klucza symetrycznego o długości 128 bitów. Jego wartość ustala się odrębnie dla każdej sesji za pomocą specjalnego protokołu SSL Handshake wykorzystującego kryptografię asymetryczną. Protokół SSL zapewnia trzy istotne z punktu widzenia ochrony danych osobowych elementy: prywatność, integralność i autoryzację.

Bezpieczeństwo danych osobowych użytkowników Internetu - zalecane standardy

Stając się czynnym użytkownikiem Internetu, tj. takim, który nie tylko biernie przegląda to, co

udostępnili inni, ale takim, który próbuje wyrażać swoje opinie, bierze udział w grupach dyskusyjnych, redaguje własny serwis informacyjny, itp. należy mieć na uwadze to, że w społeczności Internetowej, tak jak w każdej grupie obowiązują pewne zasady. Zasady te wytyczane są przez ogólnie przyjęte normy zarówno obyczajowe jak i prawne. Czyny zabronione poza Internetem, są również niedozwolone w Internecie. Jeśli na problem ten spojrzymy pod katem ochrony danych osobowych, musimy mieć świadomość, że prawa osób, których dane są przetwarzane oraz obowiązki administratorów danych w pełni odnoszą się do usług Internetowych i administrujących nimi podmiotów. Można zaryzykować nawet stwierdzenie, że niektóre z obowiązków administratora danych w przypadku internetowego przetwarzania danych nabierają szczególnego znaczenia. Jest ono proporcjonalne do zagrożeń na jakie dane te są narażone oraz obszaru ich udostępnienia. Administratorzy stron internetowych, którzy w jakikolwiek sposób za ich pośrednictwem próbują pozyskiwać informacje o odwiedzających je osobach szczególną uwagę powinni zwrócić na obowiązek informacyjny wynikający z art. 32 ustawy o ochronie danych osobowych. Administratorzy zaś, którzy wprost wykorzystują Internet do pozyskiwania danych osobowych zobowiązani są przede wszystkim do:

- Stosowania kryptograficznej ochrony danych podczas transmisji,
- Zapewnienia autoryzacji źródła ich pozyskania,
- Skutecznego zabezpieczenia pozyskanych danych przed nieautoryzowanym dostępem, ujawnieniem lub zniszczeniem.

Pomimo, że Polska ustawa o ochronie danych osobowych [5] ani wydane do niej rozporządzenia wykonawcze nie precyzują wprost warunków, jakie powinny spełniać systemy informatyczne służące do przetwarzania danych w Internecie, to większość wynika z ogólnych zapisów ustawy oraz rozporządzenia. We właściwym sformułowaniu warunków, jakim powinny odpowiadać strony WWW oraz inne systemy Internetowe służące do przetwarzania danych osobowych bardzo przydatne są zalecenia sformułowane przez Radę Europy w 1999 r. [21], zalecenia OECD [22] oraz opracowania rzeczników ochrony danych osobowych Kanady i Australii [23, 24]. Formułowane tam zasady to przede wszystkim:

a) Obowiązek określenia tożsamości podmiotu odpowiedzialnego za administrowanie danym systemem (stroną WWW) - użytkownik powinien być informowany o jego siedzibie i prawnej formie działalności,
b) Zasada automatycznego powiadamiania użytkownika o wszystkich zbieranych o nim danych w trakcie korzystania z sieci,
c) Zasada zapewniania użytkownikowi, którego dane zebrano, dostępu do jego danych w późniejszym okresie,
d) Zasada takiej konstrukcji systemu internetowego, aby zapewniał on użytkownikowi możliwość wyboru zakresu przekazywanych danych,
e) Zasada pełnej i ciągłej informacji użytkownika - na dostawcy usług internetowych i autorach stron internetowych spoczywa obowiązek informowania użytkownika o:
   - Zagrożeniach dla ochrony danych osobowych związanych z korzystaniem z sieci komputerowych,
   - Technicznych środkach ograniczających niebezpieczeństwa związane z przesyłaniem i modyfikowaniem danych w sieciach (np. kodowanie, podpis elektroniczny),
   - Możliwości korzystania z Internetu anonimowo lub z wykorzystaniem pseudonimu,
h) Zasada ciągłej prezentacji polityki ochrony prywatności - autorzy stron internetowych za

pośrednictwem, których następuje jakiekolwiek przetwarzanie danych osobowych powinni zadbać o to, aby na stronie tej było wyraźnie widoczne odesłanie do informacji o stosowanych zasadach przetwarzania danych osobowych, warunkach anonimowego korzystania oraz warunkach i narzędziach umożliwiającej użytkownikowi dostęp do własnych danych,

i) Zapewnienie jednostce, której dane dotyczą możliwości sprzeciwu wobec transakcji jego danymi,

j) Zapewnienie sprawnych procedur rozstrzygania sporów, jakie mogą powstać pomiędzy administratorem a osobą, której dane dotyczą.

Z większością wyżej sformułowanych zasad zgodna jest również organizacja World Wide Web Consortium [W3W], zrzeszająca 250 organizacji. W wydanym pod końcu 1998 r. projekcie Platform for Privacy Preferences Project [P3P] organizacja ta podkreśliła konie-czność poinformowania użytkownika w przejrzystej i zrozumiałej dla niego formie o zastoso-wanych sposobach ochrony prywatności. Podobne stanowisko odnoszące się do zasad ochrony danych osobowych w systemach Internetowych i stron WWW zajęła Grupa Robocza zajmująca się ochrona danych osobowych w telekomunikacji [26].

Pieniądz elektroniczny

Stosowane powszechnie usługi rozliczeń w handlu elektronicznym bazujące na wykorzystaniu kart płatniczych nie w pełni okazują się bezpieczne. Podczas zawierania transakcji, w celu dokonania za ich pomocą płatności niezbędne jest podanie danych osobowych oraz numeru karty kredytowej. Dane te przesyłane są w sieci Internet a następnie przechowywane na komputerze dostawcy towaru, gdzie narażone są na nieautoryzowane przetwarzanie [27, 28]. Wynika to często z braku dostosowania się stron świadczących takie usługi do zalecanych standardów. Niektóre z nich bowiem jak np. standard Secure Electronic Transaction (SET) opracowany przez organizacje płatnicze MasterCard i VISA we współpracy z IBM, Microsoft i Netscape są dość kosztowne w eksploatacji. Stąd też nieustannie poszukiwane są próby innych rozwiązań.

Dążąc do zachowania prywatności w handlu elektronicznym w wielu rozwiązaniach, dla transakcji o niewielkich wartościach próbuje się naśladować sprawdzone metody handlu tradycyjnego, w których płatności realizowane są pieniądzem tradycyjnym. Główną cechą takich transakcji ma być anonimowość. Stosowany do wzajemnych rozliczeń pieniądz tradycyjny jest anonimowy. Nie zawiera on informacji do jakich transakcji i przez kogo był wcześniej używany. Takimi samymi cechami powinien charakteryzować się pieniądz elektroniczny. Rozwiązania takie są już przygotowywane. Należą do nich miedzy innymi takie projekty jak eCash, NetCash oraz CyberCashe. Niektóre z nich oferowane są już komercyjnie. Rozwiązanie eCash będące produktem firmy Monneta oferowany jest np. przez Mark Twain Bank of St Louis (USA), Deutshe Bank oraz Bank Austria. Z wyjaśnień prezentowanych przez firmę Monneta, producenta eCash na stronie internetowej o adresie www.digicash.com/solutions wynika, że rozwiązanie to w celu wykonywania płatności nie wymaga podawania danych osobowych użytkownika.

Pieniądz elektroniczny w swej istocie jest produktem wysoko zaawansowanej matematycznej obróbki danych. Gotowy do użycia jest porcją informacji zapisaną w postaci ciągu bitów - podstawowych jednostek informacji komputerowej. Ciąg taki utożsamiany jest z przypisaną mu wartością. Jego właściwe użycie do realizowania zobowiązań dotąd nie ujawnia tożsamości osoby, która się nim posługuje, dopóki jego właściciel nie będzie próbował użyć go wielokrotnie. W przypadku oszustwa, gdy ten sam pieniądz zostanie użyty do wykonania następnej płatności, osoba, która go użyła zostanie przez bank ujawniona.

Literatura:

4. Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.; (Dz. U. 1997, 78, 483); Art. 47, 51.

5. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych; (Dz. U. 1997. 133. 833);

6. Ustawa z dnia 5 grudnia 1996 r. O zawodzie lekarza; (Dz. U. 1997. 28.152); Art. 31;

7. Ustawa z dnia 12 maja 2000 r Prawo telekomunikacyjne (Dz. U. 2000. 73. 852); Art. 67-71.

8. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. 1997. 140. 939); Art. 104.

9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych, jakim powinny odpowiadać 10. urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. 1998. 80. 521).

11. Norma PN-I-02000:1998 Technika Informatyczna - Zabezpieczenia w systemach informatycznych - Terminologia,

12. Norma PN-I-13335-1:1999 - Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych.

13. Norma międzynarodowa ISO/IEC 15408-1 Information technology - Security-techniques - Evaluation criteria for IT security.

14. Bell Labs Technical Journal. Tom 5, nr 1, styczeń-marzec 2000. Dostępny w Internecie pod adresem: www.lucent.com/minds/techjournals/.

15. Blumenthal D. J; "Pod nadzorem światła" w: Świat nauki, Marzec 2001.

16. "Strzeż się" w: Net - Magazyn użytkowników Internetu; Nr 4(13) kwiecień 2001.

17. Behrens D., Daszkiewicz K., Hajduk R., Sengstack J.; "Szpieg w pececie" w PC World Komputer 11/2000

18. Dybiec P.; Usługi lokalizacyjne w sieciach GSM, w: tele.net.forum marzec 02/2001.

19. Haag D.; publikacja internetowa pod adresem: www.federalcourts.com/federalcourt/ce_feb242000.html.

20. Matyja O.; "Sieci otwarte (na oścież)", w: Mat. Szkol."Infrastruktura Klucza Publicznego (PKI)", Instytut Matematyki PAN, 25-26 październik 2000.

21. Brown B.; "Biometric Evolution" w: PC Magazine, May 3, 1999.

22. Kuliga R.; "Praktyka zabezpieczania dokumentów", w: Software 2.0 nr 2/2001

23. Machnacz A.; "Zagrożenia bezpieczeństwa sieci i systemów teleinformatycznych" w: Mat. Konf. IT.SECURE 2000 Bezpieczeństwo - być 24. na bieżąco, Konferencja, Warszawa 18-19 października 2000.

25. Frasunek P.; "Podstępna technologia - konie trojańskie" w: Software 2.0 Nr 09/2000(96).

26. "GUIDELINES for the protection of individuals with regard to the collection and processing of personal data on information highways" - Rekomendacja Rady Europy R 99(5) z 23 lutego 1999 r. dotycząca ochrony prywatności w Internecie.

27. "Recomendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce" - Rekomendacja dotycząca wytycznych na rzecz ochrony konsumenta w kontekście handlu elektronicznego, z 9 grudnia 1999 r.

28. Cavoukian A., Crompton M.; Web Seals: A Reviev of Online Privacy Programs; A Joint Project of The Office of the Information and Privacy Commissioner/Ontario and The Office of the Federal Privacy Commissioner of Australia: Proc. of the 22nd International Conference on Privacy and Personal Data Protection, Venice, September 2000.

29. "Australia s Commissioner publishes web guidance", in:Privacy Laws & Business, No 54 July 2000.

30. "The Guidelines on Workplace e-mail, Web browsing", na stronach Internetowych www.privacy.gov.au.

31. International Working Group on Data Protection in Telecommunications; "Common Position regarding Online Profiles on the Internet" adopted at the 27th meeting of the Working Group on 4/5 May 2000 in Rethymnon / Crete (www.datenscutz-berlin.de/doc/int/iwgdpt/info27.htm).

32. Jakubski K.J.; "Sieci komputerowe a przestępczość 33. ", w:Mat. III Forum Teleinformatyki, Legionowo 1997.

34. J. Kosiński, "Carding - studium przypadku"; w: Mat. Konf. IT.SECURE 2000 Bezpieczeństwo - być 35. na bieżąco, Konferencja, Warszawa 18-19 października 2000.

36. Schneider B.; Ochrona poczty elektronicznej, WNT Warszawa 1996.

37. Szafrański M.; "Technologie sieci - Zagęszczenie w powietrzu"; w: Computerworld, Nr 15/475, 9 kwietnia 2001