ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: INFORMATYKA z. 36 Nr kol. 1414

Grzegorz FILIPCZYK
Politechnika Śląska, Instytut Informatyki

WYBRANE ZAGADNIENIA USTAWOWEJ OCHRONY DANYCH OSOBOWYCH NA PRZYKŁADZIE PROBLEMÓW WYSTĘPUJĄCYCH W URZĘDZIE MIASTA

Streszczenie. Artykuł obejmuje wybrane zagadnienia dopasowania systemu informatycznego instytucji samorządowej do wymogów stawianych przez *"Ustawę o ochronie danych osobowych"*. Dotyka takich problemów, jak zagadnienia prawne podejmowanych działań, wytyczne będące implikacją ustawy oraz proponowane sposoby ich realizacji na przykładzie Urzędu Miasta Piekary Śląskie.

CHOOSEN ASPECTS OF LAW IMPLICATED PERSONAL DATA SECURITY BASED ON PROBLEMS COMMON IN COMMUNITY

Summary. Article that is presented to You, was prepared in cooperation with Piekary Śląskie community. It covers questions relevant to the matter of law based security of personal data. It touches on such subjects as analysis of law reality and ways of implicated activities fulfilment.

1. Realia prawne podejmowanych działań

Powstała 29 sierpnia 1997 roku *"Ustawa o ochronie danych osobowych"* wraz z przyległymi rozporządzeniami Ministra Spraw Wewnętrznych i Administracji rozszerza w odniesieniu do jednostek samorządu terytorialnego oraz innych organów władzy państwowej obowiązek ochrony podstawowych dóbr osobistych na każdy zestaw danych mogący jednoznacznie zidentyfikować osobę fizyczną. Operacjom implikowanym ustawą podlega każdy zbiór danych osobowych, noszący znamiona uporządkowania, co wg uzyskanej opinii prawnej oznacza w skrajnym przypadku sporządzoną w dowolnym edytorze posortowaną listę osób. Zagadnienia informatyczne częściowo precyzuje *"Rozporządzenie Ministra Spraw*

Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych". W rozporządzeniu tym dość luźno używane są pojęcia przetwarzania, gromadzenia i wykorzystywania danych, co przy braku jasnej wykładni prawnej powoduje powstanie problemu niejednoznacznej interpretacji. Istotne fakty wynikające z zapisów ustawy są następujące:

- Konieczne jest geograficzne i logiczne określenie obszarów przetwarzania danych osobowych oraz sprecyzowania procedur zbierania i obróbki danych.
- Rozporządzenie wymusza takie dostosowanie oprogramowania, żeby możliwe było jednoznaczne określenie osoby wprowadzającej czyjeś dane osobowe po raz pierwszy do bazy, czyli by możliwe było wykonanie tzw. stempla czasowego dla powstania rekordu z danymi konkretnej osoby.
- Każda przetwarzająca dane osoba powinna być w systemie informatycznym identyfikowana w sposób jednoznaczny, a jej działania monitorowane.
- System informatyczny winien zapewniać mechanizmy ograniczenia dostępu do bazy danych do dziennego czasu pracy (np. od 7.30 do 15.30).
- System informatyczny winien być wyposażony w mechanizmy kryptograficzne chroniące poufność zebranych informacji.
- Przydzielone prawa i procedury dostępu wraz z hasłami użytkownika mają być utrzymane w tajemnicy zarówno w trakcie trwania, jak i po ustaniu stosunku pracy – dożywotnio.

Problemem dosyć istotnym jest prawna „słabość" ustawy. Częste sformułowania „jeśli przepisy odrębnych ustaw stanowią inaczej, stosuje się przepisy tych ustaw" komplikują np. procedury dostępu do baz danych zgromadzonych na serwerze (np. może wystąpić sytuacja, kiedy pomieszczenie serwera musi być dostępne dla osób trzecich, jeśli wymagają tego przepisy BHP).

2. Specyfika pracy urzędu

Niniejszy artykuł bazuje na doświadczeniach zdobytych w trakcie pracy na rzecz Urzędu Miasta Piekary Śląskie. W pracy urzędu występuje szereg obszarów, w których gromadzone są dane osobowe. Najłatwiej dokonać tu podziału geograficznego (lub organizacyjnego) zgodnie z istniejącymi w nim wydziałami:

- Wydział finansowy gromadzi dane: imię, nazwisko, adres, pesel, wiek, NIP, prowadzona działalność gospodarcza, informacje o stanie majątkowym.

- Wydział geodezji i gospodarki gruntami gromadzi dane: imię, nazwisko, adres, pesel, wiek, NIP, prowadzona działalność gospodarcza, zakres posiadanych uprawnień do wykonywania zawodu, informacje o stanie majątkowym.
- Wydział organizacji (kadr i płac) gromadzi dane: imię, nazwisko, adres, wiek, staż pracy, numer identyfikacyjny pracownika, wynagrodzenie, miejsca poprzedniego zatrudnienia, informacje o zwolnieniach lekarskich i okresach niezdolności do pracy, informacje o nagrodach i naganach, informacje o członkach rodziny.
- Wydział spraw obywatelskich gromadzi dane: imię, nazwisko, pesel, adres, dane o czasowym lub stałym zameldowaniu, o przynależności do rejonowej komendy uzupełnień wojskowych, o momencie osiągnięcia wieku poborowego, niektóre informacje o karalności lub toczących się postępowaniach sądowych, informacje o prawie wyborczym mieszkańców.
- Wydział komunikacji gromadzi dane: imię, nazwisko, pesel, uprawnienia do prowadzenia pojazdów, informacje o wstrzymaniu prawa jazdy, niektóre informacje o karalności lub toczących się postępowaniach sądowych, informacje o stanie majątkowym, informacje o uzyskanych świadectwach kwalifikacyjnych.
- Wydział architektury gromadzi dane: imię, nazwisko, pesel, adres, informacje o stanie majątkowym, niektóre informacje o karalności lub toczących się postępowaniach sądowych.

W urzędzie mogą występować różne inne jednostki organizacyjne, których nie uwzględnia powyższe zestawienie. Niekorzystnym zjawiskiem jest wielokrotne powielanie danych. Podsystemy przetwarzania poszczególnych baz danych cechują się pewną autonomicznością, ich wzajemne powiązania nie mają charakteru, który wymuszałby ich stałą synchronizację. Z drugiej strony następuje wykorzystywanie zgromadzonych danych między wydziałami, a tym samym między podsystemami: finansowy – geodezja, finansowy – kadry, finansowy – płace, geodezja – architektura, finansowy – komunikacja, przedsięwzięcia publiczne – geodezja, sprawy obywatelskie – rada miasta, sprawy obywatelskie – gospodarka lokalowa, sprawy obywatelskie – finansowy itd. Nie ma konieczności ciągłej synchronizacji podsystemów, niemniej w momencie wystąpienia konieczności musi być taka możliwość.

Bazy danych tworzone w ramach poszczególnych podsystemów są w znakomitej większości klasy dBase, poza systemem finansowo–księgowym korzystającym z aparatu oracla. Przetwarzanie ich następuje w ramach dostarczonych przez producentów programów. Każdy z programów posiada własny system kont i haseł służący do identyfikacji użytkownika i przyznania mu praw do określonych operacji nad bazą. Ponieważ ustawa mówi, że każda osoba przetwarzająca dane musi być identyfikowana w systemie w sposób jednoznaczny, to pracownik korzystający ze swojego i obcych podsystemów musi mieć kilka kont użytkownika

w ramach programów. I tak np. urzędnik wydziału finansowego w ramach poszczególnych programów winien mieć konta:

- dostępu do systemu operacyjnego (NT Workstation),
- dostępu do systemu operacyjnego sieciowego (SCO Unix),
- dostępu do systemu operacyjnego sieciowego (NetWare),
- dostępu do programu finansowo – księgowego (Oracle),
- dostępu do programu ewidencji mieszkańców (niestandardowy przez program),
- dostępu do programu ewidencji pojazdów i ich właścicieli (niestandardowy przez program),
- dostępu do programu podatkowego – od nieruchomości (niestandardowy przez program),
- dostępu do programu podatkowego – rolnego (niestandardowy przez program),
- dostępu do programu podatkowego – od prowadzonej działalności (niestandardowy przez program).

Jak widać, jest to dosyć duży zbiór, który może z czasem wzrastać. Każde z tych kont winno mieć mechanizm wymuszania zmiany hasła co najmniej raz w miesiącu, system śledzenia działalności, możliwość tworzenia tzw. stempli czasowych dla momentu pierwszego wprowadzenia danych osoby. O ile w odniesieniu do produktów potentatów światowej informatyki sprawa jest prosta – łatwo znaleźć system operacyjny czy zarządzania bazą spełniający ww. wymagania, o tyle firmy będące autorami oprogramowania specjalistycznego na rzecz urzędu nie zawsze spełniają wszystkie te warunki.

Funkcjonujące w Piekarach Śląskich bazy danych liczą około 500 MB, z czego ogromną większość stanowią zbiory typu *.dbf – możliwe do podglądnięcia i edycji prawie każdym edytorem. Występuje więc konieczność kryptograficznego zabezpieczenia ich treści. Rozwiązanie jest tu dwuetapowe:

1. Opracowanie skutecznych i szybkich sposobów szyfrowania danych na poziomie rekordów (wybór padł na funkcje mieszające).
2. Wdrożenie tych mechanizmów we współpracy z firmami będącymi autorami oprogramowania („*Ustawa o prawie autorskim (..)*" zabrania bezpośredniej, samodzielnej, nieuprawnionej ingerencji w kod programu).

I tutaj mamy do czynienia z pewnymi niuansami wynikającymi z ustawy. Nie ma sprecyzowania, co zrobić, gdy firma – autor programu nie istnieje oraz brak jest dostatecznej dokumentacji technicznej dla istniejącej w takich realiach bazy.

3. Propozycje realizacji wytycznych rozporządzenia

Wytyczne rozporządzenia można realizować na kilka sposobów. Najtańszym wydaje się być umiejętne wykorzystanie dostępnych mechanizmów systemu operacyjnego, takich jak:

- system kont i haseł z mechanizmami wymuszania ich zmian w określonych odstępach czasu,
- system ograniczania czasu i miejsca pracy,
- accounting jako narzędzie do śledzenia działań podejmowanych w systemie,
- mechanizmy praw dostępu do określonych zasobów i wykonywania działań nad zbiorami danych.

Mechanizmów takich dostarcza każdy z popularnych systemów operacyjnych sieciowych (Windows NT, NetWare, odmiany Unix'a) czy to bezpośrednio w wersji podstawowej, czy też w wersjach rozszerzonych. Ponieważ dotychczasowy system opiera się na systemie NetWare na 50 użytkowników, urząd musi ponieść koszty dodatkowych licencji (do 150 użytkowników).

Aby maksymalnie utrudnić pracownikom urzędu nieuprawniony wgląd w dane nie dotyczące sfery ich pracy, wykorzystany został mechanizm skryptów i automatycznego wylogowywania w momencie zakończenia pracy ze wskazanym programem. Szczególnie dobrze rozwiązanie to sprawdza się tam, gdzie dostęp do danych realizowany jest ze stacji bezdyskowych.

Osobnym problemem jest sprawa ochrony kryptograficznej baz. Dla zabezpieczenia przed nieuprawnionym dostępem do danych w ramach urzędu zastosowano mechanizm szyfrowania baz na poziomie rekordów. Przygotowane w Instytucie Informatyki algorytmy dostarczone zostały firmom, które są autorami oprogramowania wykorzystywanego w urzędzie i w części już zaimplementowane. Koniec prac z tym związanych planowany jest na lipiec 1999 roku. Ze względu na czas przetwarzania i dużą liczbę miejsc w kodzie programu, w których mają miejsce utrwalające dane na dysku operacje, zastosowane zostały funkcje mieszające (in. haszujące). Funkcje te stanowią dość dobry sposób zabezpieczania, a są wykonywane stosunkowo szybko.

Rozporządzenie stanowi: „§.10.1. Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, przeznaczone do likwidacji (§.10.3 naprawy), pozbawia się wcześniej zapisu tych danych (...)". Technologia odczytu danych z dysków magnetycznych posunięta jest dziś tak bardzo do przodu, że możliwy jest odczyt usuniętych danych z miejsc, w których nastąpiło nawet 10–krotne nadpisanie ich innymi danymi. Dlatego nie jest rzeczą banalną pozbawienie zapisu dysków, które były wykorzystywane np. do ustalania procedur postępowania Inspektoratu Obrony Cywilnej czy tzw. procedur NWK („na wypadek

konfliktu"). Urząd zobowiązany jest również, „Ustawą o powszechnym obowiązku obrony (..)" do przekazywania pewnych danych rejonowym komendom uzupełnień (najogólniej mówiąc – dotyczących ważnych strategicznie zasobów będących w posiadaniu podmiotów na terenie miasta). Dane zawarte w bazach należy archiwizować w określonych ustawą ramach ilościowych i czasowych oraz przechowywać przez okres, który dla konkretnego zestawu danych może dochodzić nawet do 5 lat, a jak w przypadku bazy związanej z Urzędem Stanu Cywilnego bezterminowo. Są to powody, dla których podjęte zostały badania nad możliwością wykorzystania specjalistycznego oprogramowania o nazwie SecFile, powstałego w ramach współpracy pomiędzy firmą Sotel Sp. z o.o. a Instytutem Informatyki. Postawiono sobie zadanie - doprowadzenie do bezpiecznego przechowywania archiwizowanych danych.

Oprogramowanie, o którym mowa, umożliwia szyfrowanie plików jednym z czterech algorytmów blokowych: DES (klucz 56 bitów), 3DES (klucz 168 bitów), BLOWFISH (klucz 448 bitów) oraz CAST (klucz 128 bitów). Możliwe jest szyfrowanie pojedynczych plików, ich grup lub też całych struktur katalogowych dla partycji typu FAT. Ważną rzeczą jest opcjonalna możliwość dokładnego wymazywania powierzchni dysku, którą zajmował plik oryginału – następuje 40-krotne nadpisanie. Każde zaszyfrowane archiwum dostępne jest do odszyfrowania po podaniu hasła. Produkt działa w środowisku Windows, co stwarza pewne zagrożenie – łatwo jest doprowadzić do sytuacji, gdy obok siebie znajdują się na dysku dwa pliki – oryginalny (niezaszyfrowany) i zaszyfrowany, co jest niezgodne z klasycznymi regułami kryptografii. Odszyfrowanie plików możliwe jest z wykorzystaniem klucza indywidualnego oraz awaryjnego. Bolączką okazało się wykorzystanie oprogramowania do szyfrowania zasobów sieciowych przy programie pracującym na komputerze nie będącym serwerem – przy wykorzystaniu algorytmu BLOWFISH dla sieci ethernet 10 BASE 2 z 50 stacjami klienckimi zaszyfrowanie 100 MB części bazy urzędu zajęło blisko 40 minut. Wystąpiło także klika mankamentów natury technicznej – w tym niestabilność pracy programu przy plikach o wielkościach rzędu 100 MB objawiająca się błędami sumy kontrolnej plików po odszyfrowaniu i niezgodnością zawartości plików przed i po zaszyfrowaniu. W kolejnej dostarczonej wersji programu problem ten już nie wystąpił.

Program SecFile może być stosowany do szyfrowania zawartości archiwum baz danych urzędu, a także stanu bazy na czas nieużywania jej przez urzędników (np. weekend). Jest narzędziem mocnym, wyposażonym w jedne z najlepszych mechanizmów kryptograficznych. Wadą programu jest jego związanie z pojedynczym dyskiem przez mechanizm autoryzacji praw licencyjnych - nie jest możliwe przeniesienie programu na komputer inny niż ten, na którym został pierwotnie zainstalowany.

Uzupełnieniem poziomu bezpieczeństwa dostarczanego przez SecFile są zaszyte w kod oprogramowania specjalistycznego mechanizmy tzw. funkcje haszujące (in. mieszające) stosowane przy zapisie rekordów z danymi osobowymi.

4. Wnioski i cele na przyszłość

Prawidłowe wprowadzenie zapisów ustawy wymaga stosowania metod kryptograficznych, współpracy z firmami autorskimi oraz modernizacji logicznej organizacji systemu komputerowego (systemu kont i uprawnień). W wyniku reform samorządowych nastąpiło zejście szeregu zadań publicznych na poziom instytucji samorządowych, co spowodowało konieczność rozbudowy niektórych urzędów, w tym omawianego urzędu miasta Piekary Śląskie. Obecnie urząd ten mieści się w dwóch budynkach oddalonych od siebie o około 200 metrów. Oba budynki posiadają lokalną sieć komputerową. Istnieje projekt połączenia (ściślej kilka projektów) obu budynków. Poszczególne wydziały są posiadaczami „swoich baz" w ramach podsystemów. Całość zbioru danych urzędu należy jednak już traktować jak bazę rozproszoną. Istotne znaczenie ma tu fakt postępującej integracji logicznej podsystemów, która najlepiej jest widoczna w projektowanym wdrożeniu systemu informacji terenowej SIT. Wykorzystanie zasobów poszczególnych sieci lokalnych w ramach sieci rozległej jest jak dotąd sprawą nie rozwiązaną i stanowić będzie podstawę dalszych badań.

Dosłownie w ostatniej chwili doszła kolejna grupa problemów do rozwiązania wynikających z uchwalonej w lutym 1999 roku *"Ustawy o ochronie informacji niejawnych"*.

LITERATURA

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z dnia 29 października 1997 r.
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne do przetwarzania danych osobowych, Dz.U. z dnia 30 czerwca 1998 r.

Recenzent: Dr inż. Ryszard Winiarczyk

Wpłynęło do Redakcji 8 kwietnia 1999 r.

Abstract

The common growth of computer systems that are used by communities in Poland has its reflection in law. Recording, gathering and using personal data are one of the areas where the need for law order has been noticed and implemented by adequate decree – *„Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych"*. According to that, requirements like monitoring of user work, cryptographic security, huge and 'every person' account and password mechanism must be fulfiled. The article describes how to fulfil choosen topics on the example of Piekary Śląskie community. Author shows the problems existing in community computer system, ways it works, analysis of SecFile cryptographic software and some proposal of how to use the account system.