URZĄD MIEJSKI W ŁOMIANKACH

Bezpieczna Gmina

Bezpieczeństwo danych osobowych przetwarzanych w infrastrukturze IT w sektorze publicznym

Piotr Bartoszewski
Kierownik Referatu Informatyki

Niniejszy dokument w syntetyczny sposób analizuje problemy wynikające z zapewnieniem zgodności z wymogami Ustawy o ochronie danych osobowych, szczególne w kontekście przetwarzania ich w infrastrukturze IT. Dokument zawiera propozycję rozwiązań programowych wpierających organizację bezpieczeństwa w jednostkach samorządu terytorialnego.

Spis treści

Wykaz skrótów i oznaczeń

1. **ABI** – Administrator Bezpieczeństwa Informacji
2. **ADO** – Administrator Danych Osobowych
3. **DO** – Dane osobowe
4. **UODO** - Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101 poz. 926 ze zm.)
5. **RPDO** - Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024)

Źródła

6. eduGIODO Portal Informacyjno Edukacyjny, Generalny Inspektor Danych Osobowych, https://edugiodo.giodo.gov.pl/
7. Ustawa z dnia 23 kwietnia 1964r. Kodeks cywilny (DzU nr 16, poz. 93 ze zm.)
8. Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. DzU z 1998r. nr 21 poz. 94 ze zm.)
9. Ustawa z dnia 6 czerwca 1997 Kodeks karny (DzU nr 88, poz. 553 ze zm.)
10. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tekst jedn. DzU z 2002 r. nr 101 poz. 926 ze zm.)
11. Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej (DzU nr 112, poz. 1498 ze zm.)
12. Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU nr 78, poz. 483 ze zm.)
13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024)
14. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 kwietnia 2004r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.
15. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 11 grudnia 2008r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) -wydane na podstawie art. 46 a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.
16. PN-ISO/IEC-17799:2005 Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.
17. PN-I-13335-1:1999 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.

Słowem wstępu

Dynamiczny postęp gospodarczy i technologiczny, pojawianie się innowacyjnych rozwiązań sprzętowo-programowych oraz nowe modele przetwarzania danych, nie tylko wzmogły problem przetwarzania danych osobowych, ale także spowodowały inne, niespotykane dotąd zagrożenia, mogące narazić obywateli na swoiste niebezpieczeństwo. Społeczeństwo informacyjne produkujące i przetwarzające coraz większe ilości informacji, staje również w perspektywie ochrony informacji szczególnych określanych jak dane osobowe. Takie dane Ustawa[1] określa jako „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej" (UODO art. 2 ust. 1) z kolei „osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne" (UODO art. 2 ust. 2).

Ustawa o ochronie danych osobowych jasno stwierdza, że każdy ma prawo do ochrony dotyczących go danych osobowych, a przetwarzanie danych osobowych może mieć miejsce ze względu na dobro publiczne, dobro osoby, której dane dotyczą, lub dobro osób trzecich w zakresie i trybie określonym ustawą (por. UODO art. 1 ust. 1-2). Ochrona danych osobowych wyłącznie przez jednostkę ludzką wydaje się stosunkowo trudna, dlatego obszar i zasady ochrony DO regulowane są centralnie, a przed wyzwaniem zapewnienia bezpieczeństwa przetwarzania i ochrony danych obywateli stają zarówno instytucje prywatne, jak i administracja państwowa.

Problem przetwarzania DO potęguje także to, że zakres ich przetwarzania jest stale poszerzany, gromadzonych jest coraz więcej informacji wskazujących na konkretnego obywatela, co implikuje konieczność podjęcia nowych środków i zastosowania nowoczesnych rozwiązań technologicznych służących ich ochronie. Z teorii bezpieczeństwa informacji jasno wynika, że dla zachowania bezpieczeństwa kluczowe są działania prewencyjne, a brak takich działań, skutkuje wzrostem ryzyka nieautoryzowanego dostępu do danych, naruszenia ich integralności, lub nawet kradzieży.

Niniejszy dokument stanowi studium rozwiązań technicznych i organizacyjnych służących bezpieczeństwie danych przetwarzanych w jednostce publicznej, która chcąc sprostać wymaganiom centralnych regulacji, często stoi przed wymaganiami GIODO z jednej strony, a problemami budżetowymi z drugiej.

Definicja pojęć

Jak już zostało powiedziane zakres przetwarzanych DO oraz zasady wśród których winny być one przetwarzane określa szereg przepisów w szczególności zaś Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych oraz wydane na jej postawie akty wykonawcze czyli:

[1] Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych.

- Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024)
- Rozporządzenie MSWiA z dnia 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. nr 229, poz. 1536) -wydane na podstawie art. 46 a ustawy – określa wzór zgłoszenia, który jest załącznikiem do tego rozporządzenia.
- Rozporządzenie MSWiA z dnia 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. nr 94, poz. 923) – wydane na podstawie art. 22a ustawy – określa wzory, o których mówi to rozporządzenie.

Ustawa zasadnicza stwierdza, że „organy władzy publicznej działają na podstawie i w granicach prawa" (KonstRP, art. 7). Znaczy to tyle, że podmioty publiczne mogą przetwarzać dane osobowe jedynie wtedy, gdy służy to wypełnieniu zadań, obowiązków i upoważnień określonych prawem. Tak więc, UODO definiując wytyczne przetwarzania DO razem z aktami wykonawczymi do tej ustawy stanowi trzon określający zasady i reguły przetwarzania DO. Jednak aby ukazać kompletny obraz regulacji prawnych dotyczących ochrony danych osobowych, należy wymienić pozostałe przepisy szczególne, które choć pośrednio, także regulują kwestie wykorzystywania danych osobowych:

- Ustawa z dnia 23 kwietnia 1964r. Kodeks cywilny (DzU nr 16, poz. 93 ze zm.)
- Ustawa z dnia 6 czerwca 1997 Kodeks karny (DzU nr 88, poz. 553 ze zm.)
- Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r. (DzU nr 78, poz. 483 ze zm.)
- Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (tekst jedn. DzU z 1998r. nr 21 poz. 94 ze zm.)
- Ustawa z dnia 6 września 2001r. o dostępie do informacji publicznej (DzU nr 112, poz. 1498 ze zm.)

Istotne wydaje się nadmienić, że zgodnie z art. 27 ust 1 UODO szczególną kategorią danych osobowych są tzw. dane wrażliwe, których przetwarzanie określone jest przez zasady szczególne. W zakres takich danych mogą wchodzić m.in. dane dotyczące pochodzenia rasowego, poglądów politycznych, przekonań religijnych przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów lub życia seksualnego. Istnieje zakaz przetwarzania takich danych z wyjątkiem sytuacji gdy zezwalają na to przepisy prawa (por UODO art. 17 ust 2). Jednak wśród DO przetwarzanych przez jednostki samorządu terytorialnego i organy administracji państwowej takie dane są często obecne, należy więc mieć świadomość zapewnienia szczególnego bezpieczeństwa takim

informacjom, a poprzez implementację mechanizmów ochrony konieczne jest podejmowanie działań prewencyjnych.

Choć ustawa o ochronie danych osobowych okazuje się być swoistym drogowskazem prowadzącym do bezpiecznego przetwarzania DO przez jednostki, nie wyczerpuje ona wszystkich zagadnień przetwarzania danych, a jedynie wskazuje na pewne problemy, które następnie precyzowane są we właściwych rozporządzeniach. I tak mając na uwadze przetwarzanie DO z wykorzystaniem systemów informatycznych, które z praktycznego punktu widzenia, powoduje najwięcej problemów związanych z implementacją rozwiązań, zabezpieczeń oraz realizacją wymagań urządzeń informatycznych zawiera rozporządzenie wydane na podstawie art. 39a UODO czyli Rozporządzenie MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (DzU nr 100, poz. 1024), wraz z załącznikami. To rozporządzenie ogólnie rzecz biorąc określa:

- sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2,
- podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną,
- wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

Mając powyższe na uwadze, niniejszy raport skupia się w sposób szczególny na implementacji technicznych rozwiązań i zabezpieczeń czyniącym zadość UODO i RPDO, oraz zawiera realną propozycję mechanizmów będących w zasięgu ręki jednostek samorządu terytorialnego. Bowiem poza procedurami organizacyjnymi, formalnymi upoważnieniami i mechanizmami socjologicznymi, to właśnie techniczna realizacja procesów zabezpieczeń, ma zasadniczy wpływ na bezpieczeństwo danych osobowych przetwarzanych w systemie IT.

Aby jednak w sposób kompleksowy przystąpić do omawiania powyższych zagadnień istotne wydaje się przytoczyć dodatkowo pewne definicje, które ułatwią poruszanie się w temacie i prezentację rozwiązań oraz dobrych praktyk umożliwiających sprawowanie kontroli nad wspomnianym wcześniej obszarem ochrony danych osobowych. Poniższe definicje wynikają bezpośrednio z UODO i są pewnym punktem wyjścia do dalszej analizy.

- Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
- Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

- System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
- Zabezpieczenie danych w systemie informatycznym - wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem,
- Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- Administrator danych - organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych. W praktyce jednak jest Administrator danych decyduje o celach i środkach przetwarzania danych. Między innymi może to być organ państwowy, organ samorządu terytorialnego lub państwowa albo komunalna jednostka organizacyjna.

Jako, że „administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych" (UODO art. 36 ust 1.), jest on w sposób szczególny odpowiedzialny za dane przetwarzane wewnątrz jednostki. Tak więc sposób zabezpieczenia danych winien być odpowiedni w stosunku do zagrożeń oraz kategorii danych objętych ochroną, a jakość i poziom tej ochrony powinien być adekwatny do poziomu ewentualnych zagrożeń i prawdopodobieństwa urealnienia się ryzyka (por. eduGIODO). ADO w szczególności odpowiada za zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (por. UODO Art. 36 ust 1).

Zgodnie z ustawą „administrator danych wyznacza administratora bezpieczeństwa informacji (ABI), nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności" (UODO art. 36 ust 3). Powołanie ABI jest jednak częstą praktyką, szczególnie w jednostkach liczących więcej niż kilku pracowników, a delegacja czynności przypisanych ADO osobie ABI ułatwia wdrażania procedur organizacyjnych i rozwiązań technicznych. Ważne jest jednak to, aby ABI miał pełen wachlarz uprawień i kompetencji oraz dysponował służbowymi możliwościami egzekwowania wdrażanych procedur. Warto jeszcze raz dodać, ze choć wyznaczenie ABI jest fakultatywne, w przypadku niepowołania ABI, czynności jemu przypisane wykonuje sam ADO.

Problem bezpieczeństwa danych osobowych można odnieść znacznie szerzej odnosząc się do pojęcia informacji w ogólności, oraz bezpieczeństwa jej przetwarzania przez systemy IT. Jest to określane przez dwie normy PN-ISO/IEC-17799:2005 oraz PN-I-13335-1:1999 z czego ta druga wymienia właściwości informacji, którymi są:

- Poufność – zapewnienie, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- Integralność – zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- Dostępność – zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot,
- Rozliczalność – zapewnienie, że działania podmiotu mogą być przy pisane w sposób jednoznaczny tylko temu podmiotowi,
- Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
- Niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
- Niezawodność – zapewnienie spójności oraz zamierzonych zachowań i skutków.

Przystępując do sedna niniejszego opracowania, istotne wydaje się mieć na uwadze powyższe definicje i obszar pojęć, które w jasny sposób ukazują problemy związane z przetwarzaniem informacji. Dodatkowo warto wspomnieć o potencjalnych konsekwencjach wynikających z naruszenia wymienionych wyżej aktów prawnych, a w szczególności Ustawy o ochronie danych osobowych, która w art. 52 stwierdza, że „kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku” (UODO art. 52). Z powyższego wynika wyraźnie, że samo niezapewnienie odpowiedniego poziomu zabezpieczeń, oprócz narażenia przetwarzanych DO, prowadzić może do nad wyraz poważnych konsekwencji i daleko idących skutków.

Studium rozwiązania

Ustawodawca stwierdza, że „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem” (UODO art. 36 ust 1). Aby właściwie zaplanować reakcję na tego typu zagrożenie i zaplanować działania prewencyjne, należy rozpocząć od wyboru odpowiedniego narzędzia informatycznego – środowiska, które nie tylko zabezpieczy

dostęp do pewnych zasobów, ale także umożliwi wygodne i elastyczne organizowanie polityk pracy i zasad przetwarzania danych osobowych

Przetwarzanie danych osobowych za pośrednictwem systemu teleinformatycznego implikuje kolejną cechę tego przetwarzania, bowiem wszystkie wymagania odnoście właściwości środowiska przetwarzania danych, determinują właściwości samych systemów IT. Tak więc skuteczność i ciągłość działania oraz konieczność zachowania tych właściwości jest kluczowa dla wyboru odpowiedniego rozwiązania, bowiem pewne błędy popełnione w trakcie administracji systemem lub słabości narażające system na celowe działania osób nieupoważnionych, mogą narażać bezpieczeństwo danych osobowych przetwarzanych w jednostce. „W konsekwencji, oprócz działań mających na celu ochronę przetwarzanych danych, należy zapewnić również ochronę systemu informatycznego, którego użyto do ich przetwarzania" (eduGIODO). Dlatego także przepisy wykonawcze ustawy wydane na podstawie art. 39 UODO, określają wymagania dotyczące tak polityki bezpieczeństwa, jak systemu informatycznego oraz sposobu w jaki jest on zarządzany.

Pewną sprawdzoną propozycją, wykorzystywaną z powodzeniem w wielu jednostkach samorządu terytorialnego, jest środowisko pracy oparte o rozwiązania Microsoft Windows Server, a w szczególności usługa katalogowa Active Directory, która będąc hierarchiczną bazą danych jest doskonałym punktem wyjścia do implementacji wymagań ustawy oraz aktów wykonawczych. Urząd Miejski w Łomiankach z powodzeniem wdrożył i zarządza bezpieczeństwem danych z wykorzystaniem wyżej wymienionych usług, których wdrożenie i uruchomienie nie pociąga za sobą wysokich kosztów, a administracja nie wymaga specjalistycznych kompetencji i zasobów organizacyjnych.

Przetwarzanie danych w sieci

RPDO uwzględniając kategorie przetwarzanych danych oraz zagrożenia wprowadza poziomy bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym (por. RPDO §6, ust. 1):

1. podstawowy
2. podwyższony
3. wysoki

Nie wdając się w szczegóły rozporządzenia wypada przytoczyć §6, ust. 4 RPDO, w którym stwierdza się, że poziom wysoki stosuje się wtedy, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania DO, połączone jest z siecią publiczną. Tak więc samo podłączenie jednego tylko urządzenia systemu IT, służącego do przetwarzania DO z siecią publiczną, skutkuje koniecznością wprowadzenia wysokiego poziomu bezpieczeństwa przetwarzania danych. Pociąga to za sobą konsekwencje w postaci konieczności sprostania wszystkim wymaganiom Załącznika do RPDO, takimi jak wymogi dotyczące haseł, zabezpieczeń logicznych sieci oraz kontrolę działań inicjowanych zarówno z sieci publicznej jak też z systemu informatycznego.

Referaty i wydziały, które nie stanowią logicznie wyizolowanego obszaru przetwarzania danych osobowych są znacznie bardziej narażone na ataki pochodzące z zewnątrz. Tak więc, znaczna cześć Urzędów Miejskich chcąc sprostać wymaganiom stawianym przez Rozporządzenie powinna nie tylko chronić system informatyczny służący do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem (Załącznik do RPDO pkt XII ust. 1), ale także stosować mechanizmy organizacyjne wymagane w RPDO na poziomach niższych niż wysoki.

Istnieje kilka rozwiązań dostarczanych przez Microsoft umożliwianych spełnienie wymagań Rozporządzenia, istotne jest wymieć usługę katalogową Active Directory, która pracując w infrastrukturze IT opartej o Windows Server daje możliwość centralnej implementacji zabezpieczeń lokalnych stacji roboczych i kontrolę nad tymi zabezpieczeniem, np. poprzez wymuszanie uruchomienia usługi firewall na stacjach roboczych, definicje wyjątków i konfigurację reguł. Nie sposób pominąć jednak zaawansowanej zapory filtrującą cały ruch sieciowy - Microsoft Internet Security and Acceleration Server (ISA Server), która umożliwiając ochronę sieci wewnętrznej przez zagrożeniami pochodzącymi zewnątrz stanowi zintegrowane rozwiązanie wspierające bezpieczeństwo publikacji stron internetowych oraz inne usługi takie jak routing i dostęp zdalny oraz VPN.

Mechanizmy kontroli oraz autoryzacja użytkowników

Zgodnie Załącznikiem do RPDO w systemie informatycznym oraz w infrastrukturze IT istnieje potrzeba stosowania mechanizmów kontroli dostępu do danych osobowych (Załącznik do RPDO pkt II, ust. 1). A jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, istnieje konieczność zapewnienia:

1. aby w systemie rejestrowany był odrębny identyfikator dla każdego użytkownika;
2. dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia (Załącznik do RPDO pkt II, ust. 2).

Takie mechanizmy w swej istocie chronią dane osobowe przez nieuprawnionym dostępem, nieautoryzowaną modyfikacją oraz ich zniszczeniem. Pewna funkcjonalność systemu Windows Server oraz usługi katalogowej Active Directory, zwana zasadami grupy (Group Policy Object), dostarczana przez Microsoft, kontroluje środowisko pracy kont użytkowników oraz komputerów. GPO zapewnia scentralizowane zarządzanie i konfigurację systemów operacyjnych, aplikacji i ustawień użytkowników w środowisku Active Directory. Umożliwia definiowanie i monitorowanie dostępu do poszczególnych zasobów sieciowych oraz zarządzanie nimi poprzez określanie konkretnych przydziałów do zasobów. Takie przydziały są możliwe do zdefiniowania zarówno na poziomie urządzenia, jak też na poziomie użytkownika.

Tak więc użytkownicy pracujący w środowisku Active Directory autoryzowani są za pomocą unikalnego loginu i hasła, umożliwia to egzekwowanie polityki przetwarzania danych osobowych i rozliczalność pracowników z przetwarzanych przez nich informacji. W takiej

sytuacji dostęp do zasobów sieciowych, szczególnie tych zawierających zbiory danych osobowych, może być precyzyjnie kontrolowany i monitorowany. Użytkownik bowiem uzyskując dostęp do pewnego obszaru informacji, uzyskuje jednocześnie uprawnienia określające poziom dostępu jaki został mu przydzielony (modyfikacja, odczyt, zapis etc.)

Implementacja wspomnianego wyżej środowiska opartego o technologię Windows Serwer umożliwia stosowanie mechanizmów wykluczających przydzielenie innej osobie identyfikatora użytkownika, który utracił uprawnienia do przetwarzania danych, lub uprawnienia do pracy w systemie. Warto przypomnieć, że takie wykluczenie jest konieczne ze względu na wytyczne Rozporządzenia (por. Załącznik do RPDO, pkt II, ust. 2).

Istotne wydaje się dodać, że centralne zarządzanie dostępem do zasobów zostaje również z powodzeniem stosowane do implementacji polityk scentralizowanego zarządzania dostępem do zasobów takich jak drukarki, współdzielone zasoby dyskowe, oraz dostępu do zdalnych aplikacji. Na tej podstawie można więc utworzyć kilka hermetycznych środowisk, gdzie każde z nich posiada swoiste uprawnienia, jedynie do tego obszaru przetwarzania danych jaki został określony w upoważnieniu ADO.

Bezpieczeństwo i polityka zmiany haseł

Wdrożenie środowiska Active Directory, implementacja zasad polityki bezpieczeństwa, oraz realizacja tych reguł we wspomnianym środowisku rozwiązuje także problem wymagań bezpieczeństwa dotyczących haseł które Załącznik do RPDO określa w pkt IV, ust. 2, oraz w pkt VIII, takie jak ilość i zakres znaków. Warto także dodać kolejną cechę bezpiecznego hasła, mianowicie unikanie powtarzalności haseł wstecz.

Mówiąc o wysokim poziomie bezpieczeństwa przetwarzana danych osobowych narzucone zostaje wymaganie uwierzytelniania użytkowników za pomocą hasła, które składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne. I choć zasady zmiany haseł nad wyraz często są w Urzędach realizowane poprzez reguły organizacyjne, wobec których po stronie użytkownika leży obowiązek pamiętania o cyklicznej zmianie haseł dostępu do zasobów, ich zakresu znakowego oraz powtarzalności. Niebagatelną wartość stanowi mechanizm będący rozwiązaniem systemowym, który realizowany centralnie czyni zadość wymaganiom Rozporządzenia w tym zakresie. Implementacja centralnych mechanizmów możliwa jest właśnie w środowisku Active Directory, gdzie możliwe jest określenie cykliczności zmiany haseł, stworzenie wymogów ich zakresu znakowego oraz pamiętanie haseł wstecz, wykluczając tym samym ponowne wykorzystanie tego samego hasła, co znacznie podwyższa bezpieczeństwo systemu oraz redukuje ryzyko wycieku danych logowania poza grupę upoważnionych użytkowników.

Czas reakcji na incydent

Czas reakcji na incydent wydaje się być kluczową cechą dobrze zorganizowanego systemu przetwarzania danych osobowych. I choć polityka bezpieczeństwa powinna obejmować swym zakresem wskazanie możliwych rodzajów naruszenia bezpieczeństwa (np. nieautoryzowany dostęp do zasobów, zniszczenie danych, etc.) oraz zdefiniowane

scenariusze postępowania wobec takich sytuacji, nie sposób wyczerpać wszystkie zagrożenia i możliwości na które mogą zostać narażone przetwarzane dane osobowe. Jednak chcąc nieco przybliżyć sam problem, istotne wydaje się określić przykładowy incydent powodujący kompromitację kilku, bądź wszystkich haseł systemowych używanych na stacjach roboczych. Odpowiedzią na tego typu problem z konieczności musi być zmiana wszystkich skompromitowanych haseł, co w przypadku kilkudziesięciu, bądź kilkuset komputerów może okazać się nad wyraz trudne. Jednak wykonanie takiej czynności dysponując mechanizmem przechowującym dane użytkowników w postaci centralnej bazy danych Active Directory, jest czynnością stosunkowo prostą, a wykonanie zadania wymuszenia zmiany wszystkich haseł na kilkuset komputerach trwa poniżej dziesięciu minut. Warto przytoczyć wyniki testów reakcji na tego typu incydent wykonanych przez Urząd Miejski w Łomiankach, gdzie czas reakcji działu IT na kompromitację jednego tylko hasła został skrócony o 85%, a skoro czas wymuszenia zmiany większej ilości haseł rośnie geometrycznie, oszczędności czasu są jeszcze większe, a ryzyko wycieku danych w czasie między kompromitacją hasła, a jego zmianą drastycznie maleje.

Polityka blokowania dostępu

Zaawansowane mechanizmy kontroli dostępu do zasobów dostarczane za pośrednictwem usługi Active Directory, zostają także z powodzeniem wykorzystywane do czasowego ograniczania dostępu do DO i pozostałych zasobów informacyjnych organizacji poszczególnym pracownikom. I nie chodzi tu oczywiście o samo w sobie ograniczanie dostępu do zasobów wspomnianym osobom (choć poniekąd to też stanowi pewną wartość) ale to wykluczenie wykorzystania danych do logowania przez inną osobę, co w konsekwencji skutkuje podszyciem się pod tożsamość tej pierwszej. Tak więc, użytkownicy systemu nie przebywający w pracy, czy to z powodu zwolnienia z pracy, czy przebywania na urlopie, nie mają możliwości zalogowania się do systemu, a zdefiniowane pewnych wyjątków (np. wobec kluczowego pracownika) jest możliwe na żądanie oraz jest potwierdzane każdorazowo przez naczelne kierownictwo Urzędu. Taka polityka umożliwia także kontrolowanie dostępu do zasobów organizacyjnych oraz ograniczanie go poza godzinami pracy biura, tak w godzinach nocnych jak w dni wolne od pracy. Taki mechanizm realizowany centralnie, oparty w usługę Active Directory, w znaczy sposób ogranicza możliwość ingerencji, bądź ataku wymierzonego w zasób informacyjny, wykorzystując dane konkretnej osoby.

Zabezpieczenie przed wyciekiem informacji

Scentralizowana polityka kontroli dostępu do zasobów realizowana za pośrednictwem Active Directory umożliwia implementację mechanizmów zabezpieczających dane osobowe przed ich wyciekiem poprzez nośniki zewnętrzne. Stosowanie takich mechanizmów nie tylko w formie procedur organizacyjnych, ale polityki fizycznego blokowania dostępu do urządzeń peryferyjnych takich jak dvd-rom, pamięci typu flash, dyski zewnętrzne, czy inne urządzenia mobilne, w znaczny sposób redukuje ilość niekontrolowanych kanałów wycieku informacji z jednostki. Stosowanie rozwiązania

programowego w postaci usługi Active Directory w tym względzie, znacznie ułatwia sprawowanie centralnego nadzoru nad zaimplementowanymi politykami oraz tworzenie pewnych wyjątków od tych reguł.

Centralne aktualizacje oprogramowania

Powszechnie wiadomo, że system operacyjny oraz pozostałe oprogramowanie systemu będąc w dużym stopniu narażone na ataki szkodliwych programów różnego typu, powinno być stale aktualizowane do najnowszej wersji. Utrzymywanie aktualnych wersji aplikacji systemowych i systemu operacyjnego, nie tylko minimalizuje problem luk w oprogramowaniu, ale także wyposaża system i zainstalowane oprogramowanie w nowe funkcje, które są nieobecne w wersjach starszych. Takie aktualizacje poprawiając bezpieczeństwo, oraz komfort pracy użytkownika wydają się kluczowe dla dobrze zorganizowanego systemu ochrony danych osobowych. Prowadzenie scentralizowanej polityki aktualizacji oprogramowania i systemów operacyjnych ułatwia sprawowanie kontroli nad bieżącą wersją oprogramowania, śledzenie postępów w aktualizacji i implementację nowych poprawek do wykorzystywanych aplikacji.

Kompleksowe wsparcie w obszarze aktualizacji systemu operacyjnego Windows dostarcza centralnie uruchomione usługa Windows Server Update Service (WSUS), która umożliwia administratorom systemu zarządzanie aktualizacjami i poprawkami do produktów firmy Microsoft oraz ich dystrybucję na komputery w środowisku firmowym. WSUS pobierając wybrane aktualizacje z witryny Microsoft Update, rozsyła je do komputerów w sieci lokalnej. WSUS działa jak usługa Windows Server, a uruchomienie jej nie generuje dodatkowych kosztów.

W tym miejscu problemem mogą wydać się aktualizacje aplikacji wykorzystywanych w środowisku firmowym, a jednak dostarczanych przez niezależnych producentów i dystrybutorów. Jednak i w tym miejscu, z pomocą przychodzi usługa Active Directory, w szczególności mechanizmy GPO, które umożliwiają centralną aktualizację oprogramowania znajdującego się na stacjach roboczy, lub stworzenie całego pakietu oprogramowania, które nawet bez wiedzy użytkownika końcowego zostanie zainstalowane lub zaktualizowane.

Aby określić pewien wymierny wskaźnik, warto posłużyć się badaniem przeprowadzonym przez Urząd Miejski w Łomiankach, który poddał analizie czas reakcji działu IT na lukę wykrytą w oprogramowaniu systemowym od momentu wykrycia luki do instalacji poprawki na wszystkich stacjach roboczych. We wspomnianym środowisku Urzędu Miejskiego w Łomiankach, dział IT potrzebował od 2 do 3 dni na ręczną instalację poprawki na wszystkich stacjach roboczych, po wdrożeniu mechanizmów realizowanych w środowisku Windows Serwer czas instalacji poprawki wyniósł od 5 do 10 minut.

Logowanie nieautoryzowanego dostępu

Biorąc pod uwagę właściwości informacji wyszczególnione na początku niniejszego dokumentu, uwidacznia się kolejna cecha tworząca wartość dodaną wdrożenia środowiska opartego o mechanizmy Windows Server, gdyż Active Directory umożliwia monitorowanie

nieudanych prób logowania na stację roboczą, bądź do zasobów sieciowych. Takie dane z kolei mogą dostarczyć niezmiernie ważnych informacji, gdzie, kiedy i jak próbowano uzyskać nieautoryzowany dostęp lub odgadnąć czyjeś hasło. Takie działania mogą naruszyć i często naruszają integralność systemu, więc ważne jest aby nieautoryzowane próby dostępu do stacji roboczych były stele logowane i monitorowane.

Szyfrowanie danych

Zgodnie z Załącznikiem do Rozporządzenia Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, o którym mowa w § 4 pkt 1 rozporządzenia, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych (Załącznik do RPDO pkt V). Stosowanie środków kryptograficznych na urządzeniach mobilnych jest wiec konieczne dla spełnienia wymogów Ustawy. Natomiast środowisko Windows Server wspiera takie mechanizmy i upraszcza procedury szyfrowania i ewentualnego odzyskiwania danych np. w przypadku zagubienia lub uszkodzenia klucza szyfrującego.

Rozwiązanie BitLocker zaimplementowane jest w systemach operacyjnych dostarczanych przez Microsoft, pozwala ono na kryptograficzną ochronę danych na dyskach poszczególnych komputerów. Uruchomienie tego rozwiązania w środowisku firmowym Windows Server umożliwia nie tylko centralnie zarządzania szyfrowaniem dysków , ale także daje możliwość odzyskiwania kluczy szyfrujących przechowywanych centralnie (a nie lokalnie) w Active Directory. Co jak wspomniano jest kluczowe w sytuacji uszkodzenia dysku, komputera lub kradzieży któregoś z dysków na którym właśnie przechowywany był klucz.

Bezpieczna poczta elektroniczna

Przetwarzanie danych oraz ich przesyłanie za pośrednictwem poczty elektronicznej, również stanowi pewnego rodzaju zagrożenie z jednej strony, a wyzwanie z drugiej, bowiem te same zagadnienia i problemy, które miały miejsce w poprzednich punktach takie jak zmiana i reguły haseł, wymuszanie zmiany hasła, blokowanie dostępu oraz aktualizacja oprogramowanie poczty, powinny dotyczyć także systemu poczty elektrycznej. Owe mechanizmy można implementować w sposób odrębny, bądź zintegrować z funkcjonującym środowiskiem Windows Server, w którym jak wspominano są one zaimplementowane i gotowe do wykorzystania. Wdrożenie Microsoft Exchange Server wydaje się znakomitym rozwiązaniem, bowiem biorąc pod uwagę kompleksową realizację usług w środowisku Windows Server, zdecydowana większość wymagań ustawowych dotyczących przetwarzania danych zostaje przekazana usłudze Active Directory, a serwer poczty jedynie z nich korzysta, dodatkowo zapewniając mechanizmy szyfrujące, wyszukujące, gromadzące dane oraz filtry antyspamowe, będące przydatne w dostępie do Danych Osobowych, nie wymaganych jednak Ustawą. Istotne wydaje się także dodać, że we wspomnianym środowisku poczty elektrycznej komunikacja urządzeń mobilnych z systemem poczty elektronicznej jest

szyfrowana, co znacznie podnosi bezpieczeństwo samej transmisji, jak też redukuje ryzyko przechwycenia przesyłanych treści przez osoby nieuprawnione.

Podsumowanie

Ustawa o ochronie danych osobowych oraz wydane na jej podstawie akty wykonawcze stawiają przez jednostkami samorządu terytorialnego wyzwania, które są kluczowe dla obywateli, gdyż to właśnie ich dane osobowe są przez samorządy przetwarzane. Dynamiczny rozwój technik informatycznych i metod socjologicznych pozwala jednak na coraz precyzyjniej wymierzone ataki, skierowane na konkretny zasób, bądź zbiór danych. Właściwe zabezpieczenie przechowywanym przez Urząd Informacji winno opierać się na dwóch filarach, którymi są po pierwsze procedury organizacyjne umożliwiające definicję procesów przetwarzania danych, po drugie zaś rozwiązania programowane, które uniemożliwiają nieautoryzowany dostęp do zasobów Urzędu. Budowa środowiska opartego o Windows Server i usługę Active Directory umożliwia stworzenie spójnego systemu bezpieczeństwa, dającego możliwość centralnej administracji regułami i zasadami na stacjach roboczych pracujących w sieci. Budowa środowiska Active Directory poprzez szczególny model licencjonowania dla jednostek samorządu terytorialnego jest ekonomiczna kosztowo, a poprzez intuicyjne interfejsy administracyjne daje znaczny wzrost wydajności Działu IT.

Tak zbudowane środowisko funkcjonuje z powodzeniem od wielu miesięcy w Urzędzie Miejskim w Łomiankach, a taka optymalizacja środowiska informatycznego, spowodowała znaczne oszczędności czasu, co z kolei umożliwiło uwolnienie zasobów ludzkich działu IT z bieżących zadań administracyjnych i przydzielenie ich do kluczowych, realizowanych przez Urząd projektów.