Zabezpieczenie dostępu do informacji w tym do danych osobowych

na przykładzie oprogramowania RCP 5.0 Enterprise firmy Polsystem

Tomasz Adamski
Polsystem

Ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. (Dz.U. 2015, poz. 2135 z późn. zm.) zawiera wymagania i obowiązki względem systemów informatycznych przetwarzających dane osobowe oraz dotyczące administratorów danych osobowych (ADO) i administratorów bezpieczeństwa informacji (ABI). Ustawa definiuje system informatyczny jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Natomiast przetwarzanie danych to dowolne operacje wykonywane na danych osobowych, np. ich zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, zwłaszcza te, które wykonuje się w systemach informatycznych.

Systemy klasy RCP i KD oraz inne systemy informatyczne przetwarzające dane osobowe powinny spełniać wiele wymogów, w tym tych dotyczących zabezpieczeń poziomu technicznego programów pod kątem ochrony danych osobowych. Niestety, wielu krajowych dostawców i integratorów implementujących rozwiązania niskobudżetowe często nie zdaje sobie sprawy z powagi sytuacji i ewentualnych konsekwencji z tego wynikających zarówno dla nich, jak i podmiotów korzystających z rozwiązań, które nie spełniają wymogów ustawy o ochronie danych osobowych.

Bezpieczeństwo baz danych

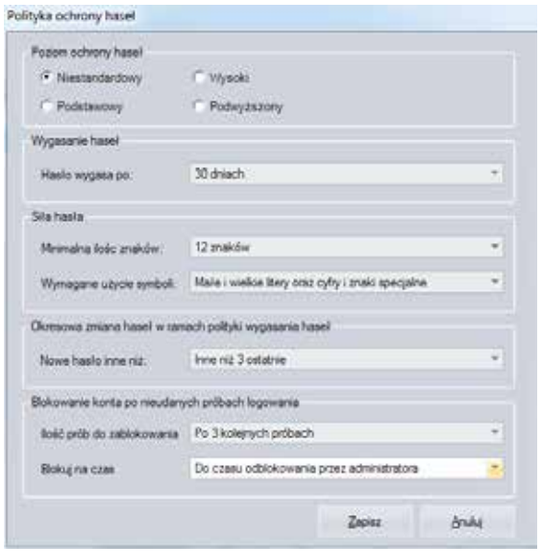
Profesjonalne rozwiązania do ewidencji czasu pracy i kontroli dostępu są najczęściej oparte na bezpiecznych, oczywiście przy odpowiedniej ich konfiguracji, relacyjnych bazach danych Microsoft SQL. Niskobudżetowe, „pudełkowe" systemy często korzystają z plikowych baz danych, których strukturę i zawartość można szybko odszyfrować i odczytać przy użyciu łatwo dostępnych narzędzi.

Szyfrowanie połączenia między aplikacją RCP/KD a bazą danych zapewnia środowisko MSSQL, które ma mechanizmy umożliwiające szyfrowanie protokołu komunikacyjnego z użyciem 40- lub 128-bitowego klucza – certyfikatu SSL (Secure Sockets Layer). Oczywiście, jeżeli owo szyfrowanie samego protokołu komunikacyjnego byłoby zbyt słabym zabezpieczeniem, np. ze względu na wysokie wymogi poszczególnych korporacji, środowisko bazodanowe można osadzić na wirtualnym serwerze, z którym połączenie może być realizowane za pomocą bezpiecznego tunelu VPN (Virtual Private Network).

Polityka ochrony haseł

Skoncentrujmy się jednak na bezpieczeństwie dostępu do danych osobowych, poprzez dedykowane do tego aplikacje – oprogramowanie RCP i KD 5.0 Enterprise firmy Polsystem. Logowanie użytkowników programu oczywiście jest zabezpieczone hasłem. Ciekawą z punktu widzenia administratorów systemu RCP funkcjonalnością jest możliwość autoryzacji bez podawania hasła użytkownika (z użyciem nazwy komputera – wykorzystując usługi Active Directory). Jeżeli natomiast uwierzytelnienie użytkowników odbywa się za pośrednictwem nazwy użytkownika (loginu) i hasła, administrator może włączyć w systemie restrykcyjną „politykę ochrony haseł" wybierając ją spośród kilku dostępnych wariantów lub skonfigurować według własnego uznania zasady tworzenia i ochrony haseł (rys. 1).

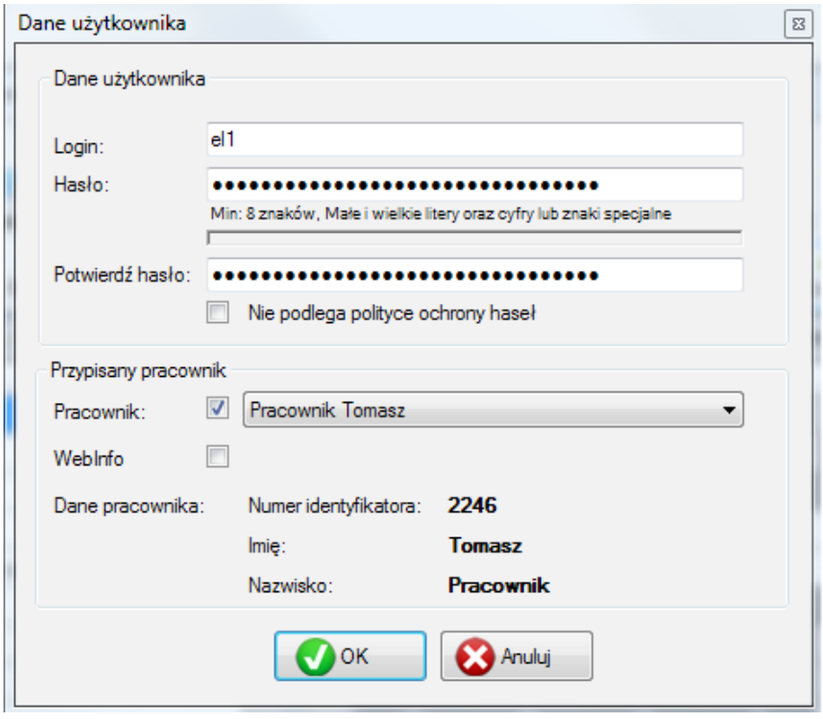
Mamy tutaj wiele konfigurowalnych możliwości, takich jak termin ważności hasła, jego minimalna długość, rodzaj i typ znaków, jakie powinny zostać użyte, czy walidację nowych haseł z hasłami wcześniej użytymi.



Rys. 1. Tworzenie reguł ochrony haseł

Administrator na etapie tworzenia użytkownika (operatora) oprogramowania może, czy wręcz powinien z punktu widzenia ochrony danych osobowych, przypisać danego użytkownika do konkretnej osoby (z imienia i nazwiska), co przedstawia rys. 2. Jeżeli osoba, której konto w systemie tworzymy jest pracownikiem naszej organizacji, będzie dostępna na liście rozwijanej, co umożliwi jej szybkie przypisanie.

Dodatkowo, ze względów bezpieczeństwa system może kontrolować długość sesji użytkowników oprogramowania i jeżeli nie wykryje aktywności użytkownika przez określony czas, co może świadczyć o opuszczeniu stanowiska komputerowego przez operatora, automatycznie zakończy sesję i wyloguje użytkownika z systemu, tak by niepowołane osoby nie miały dostępu do aplikacji – wymagane będzie wówczas ponowne uwierzytelnienie użytkownika. Jeżeli polityka haseł przewiduje kontrolę poprawności logowania użytkowników, operator oprogramowania, który popełni zdefiniowaną liczbę błędów logowania, zostanie zablokowany na określony czas lub do momentu ingerencji administratora.



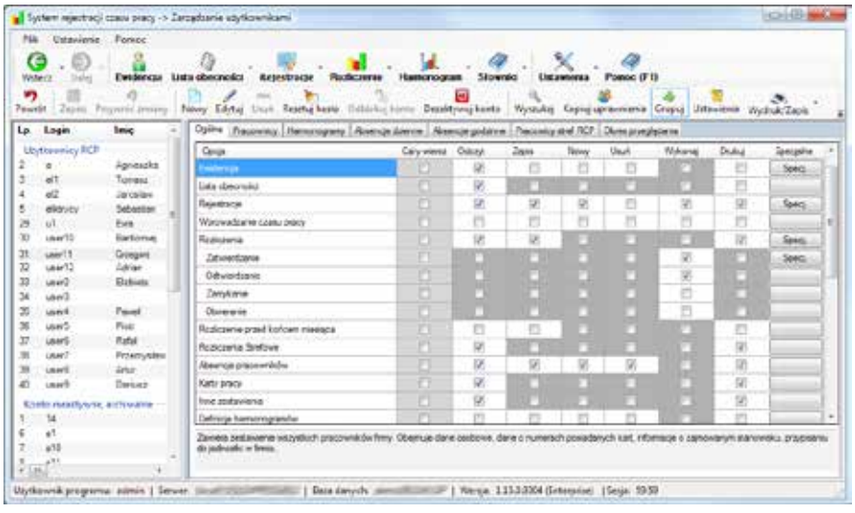
Rys. 2. Administracja – przypisywanie operatora do właściciela konta

Rys. 3. Informacja o blokadzie konta w wyniku błędnej autoryzacji

Konfiguracja uprawnień

Dostęp użytkowników do funkcji programu RCP także może być ograniczony przez administratora. Ograniczenia mogą być nakładane na poszczególne funkcje, np. na przeglądanie, modyfikacje, wprowadzanie nowych danych, usuwanie, wydruki, oraz operacje dostępne do wykonania. Ponadto można ograniczyć uprawnienia poszczególnych użytkowników do danych znajdujących się w systemie, takich jak pracownicy; harmonogramy; absencje czy okres przeglądania (rys. 4).

Po odpowiedniej konfiguracji uprawnień, manager, kierownik wydziału lub mistrz produkcji może mieć dostęp tylko do danych tych pracowników, którzy mu podlegają. Oczywiście istnieje także możliwość połączenia uprawnień do pracowników w sposób automatyczny – z wykorzystaniem hierarchicznej struktury zakładu. Wówczas po przypisaniu pracownika do wybranego wydziału lub grupy, osoba zarządzająca danym zbiorem pracowników otrzyma automatycznie uprawnienie do nowo dodanej osoby.



Rys. 4. Administracja – definiowanie ról użytkowników

Dostęp do danych osobowych i ich modyfikacja

Operacje wykonywane przez operatorów oprogramowania są automatycznie zapisywane w bazie danych (logowane) zarówno na płaszczyźnie rozliczeń pracowników, za którymi idą kwestie finansowe (system umożliwia automatyczne generowanie listy pracowników z czasem przez nich przepracowanym w podziale na wymagane do naliczenia płac w systemie płacowym składniki rozliczeń), jak i na płaszczyźnie dostępu i modyfikacji danych osobowych. Dzięki temu możliwe

jest generowanie różnych raportów dot. dostępu i edycji informacji przechowywanych w bazie danych.

Z punktu widzenia administratorów bezpieczeństwa informacji (ABI) oraz administratorów danych osobowych (ADO), bardzo istotne będą raporty o dostępie użytkowników systemu do danych osobowych (rys. 6) oraz o wykonywanych przez nich operacjach na tych danych (rys. 5).

Dlaczego warto wybrać Polsystem

Przedstawione powyżej funkcje oprogramowania RCP firmy Polsystem stanowią jedynie drobny fragment jego możliwości, który koncentruje się na szeroko rozumianym bezpieczeństwie danych.

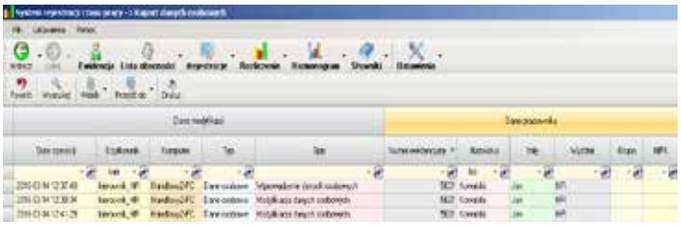
Programowe narzędzia Polsystem doceniło wielu klientów z różnych branż, działających zarówno w sektorze jednostek budżetowych, jak i w sektorze przedsiębiorstw zatrudniających od kilkudziesięciu do kilku tysięcy osób. Wśród kluczowych rozwiązań Polsystemu, o których nie było mowy powyżej, należałoby wymienić chociażby:

- Zgodność ze zmianami przepisów Kodeksu Pracy.
- Obsługa wielu systemów pracy.
- Możliwość definiowania indywidualnego systemu rozliczania dla każdego pracownika.
- Obsługa różnych okresów rozliczeniowych czasu pracy, w tym rocznego.
- Szybkość działania, rozliczenie czasu pracy i generowanie raportu trwa do kilkunastu sekund, przy czym prędkość działania nie jest zależna od stacji roboczej, lecz od serwera bazy danych RCP.
- Funkcjonalna nawigacja i proste w obsłudze, czytelne menu.
- Opcjonalna, anglojęzyczna wersja programu.
- Zarządzanie współdzielonymi profilami i widokami użytkownika.
- Predefiniowane panele informacyjne dla pracowników przez aplikację WebInfo, dostępną przez przeglądarkę internetową.
- Import danych dotyczących pracowników z systemów HR, np. lista pracowników i kody nieobecności.
- Eksport danych i raportów do systemów kadrowo-płacowych – także w oparciu o rozwiązania działające w trybie on-line.

Wspomniany powyżej program RCP 5.0 Enterprise jest podstawową aplikacją całego systemu. Jego funkcjonalność może zostać znacznie poszerzona przez rozbudowę o takie dodatkowe moduły jak:

- Zlecenia 5.0 – program do ewidencji i rozliczania operacji, zadań czy zleceń wykonywanych przez pracowników.
- Kontrola Dostępu 5.0 – zaawansowane oprogramowanie kontroli dostępu, które umożliwia między innymi:
  - planowanie stref bezpieczeństwa (także graficzne)
  - poziomy uprawnień
  - definiowanie harmonogramów KD
  - raportowanie ruchu osób i listy obecności dla potrzeb ewakuacyjnych.
- Księga gości – jest modułem oprogramowania KD 5.0 i oferuje m.in. takie funkcjonalności:
  - zarządzanie przepustkami dla gości i kontrahentów oraz ewidencja wydanych przepustek
  - możliwość wydawania pracownikom kart tymczasowych
  - ewidencja pojazdów poruszających się po obiekcie
  - obsługa skanerów dokumentów tożsamości oraz czytników kart, co znacznie skraca i upraszcza proces wydawania przepustek.
- Kantyna – program do kontroli wydawania i zarządzania posiłkami wydawanymi w stołówce zakładowej. Pozwala w szybki i przyjazny sposób określać uprawnienia pracowników do posiłków oraz zarządzać ich wydawaniem.
- WebInfo – pełni funkcję kiosku informacyjnego, w którym pracownicy mogą sprawdzić takie dane, jak liczba dni urlopu do wykorzystania, terminy badań i szkoleń, grafik, jaki został im przydzielony, ich rozliczenia za miniony okres (w tym przepracowywane nadgodziny i liczba godzin do odbioru).
- e-WU (Elektroniczne Wnioski Urlopowe) jest w pełni elektronicznym narzędziem wspomagającym pracownika w samodzielnym planowaniu terminów urlopu oraz dział personalny i kadrę zarządzającą w podejmowaniu decyzji dotyczących urlopów pracowników firmy.

Więcej informacji na temat produktów firmy Polsystem na www.polsystem.pl



Rys. 5. Raport wprowadzonych zmian w danych osobowych

INFORMACJA O DANYCH OSOBOWYCH

A. Dane personalne	
Imię:	Jan
Nazwisko:	Kowalski
Drugie Imię:	Tadeusz
Drugie nazwisko:	-
Pesel:	[redacted]
Płeć:	Mężczyzna
Numer identyfikatora:	5631
NIP:	
Czy wprowadzono wizerunek (zdjęcie):	Nie
Data pierwszego wprowadzenia:	2016-03-14 12:37:48
Użytkownik:	kierownik_HR
Data ostatniej modyfikacji:	2016-03-14 12:42:52
Użytkownik:	kierownik_HR
B. Dane adresowe	
Ulica:	Francuska
Nr domu:	92
Kod pocztowy:	54-405
Miasto:	Wrocław
Telefon:	-
E-mail:	-
Data pierwszego wprowadzenia:	2016-03-14 12:41:29
Użytkownik:	kierownik_HR
Data ostatniej modyfikacji:	2016-03-14 12:41:51
Użytkownik:	kierownik_HR
C. Informacje o udostępnianiu	
Dostęp do danych mają użytkownicy:	kierownik_HR

Rys. 6. Raport o udostępnieniu danych osobowych użytkownikom