Oracle Identity Govenrance

Standaryzacja procesu zarządzania użytkownikiem i jego uprawnieniami

Euler Sp. z o.o.
ul. Obrońców Tobruku 31A/130
01-494 Warszawa
e-mail: euler@euler.pl
http://www.euler.pl

Jak chronić informację?

Wstęp

Aktywa są najważniejszymi obiektami, jakie chroni każde przedsiębiorstwo. Aktywem jest sprzęt za pomocą, którego wytwarzane są towary, aktywem jest nieruchomość, w końcu aktywem jest informacja. To informacja jest najistotniejszym aktywem, jakie każda firma powinna chronić adekwatnie do jej wartości. O ochronie informacji mówmy w kilku obszarach:

- Ochrona poufności informacji – chcemy mieć pewność, że tylko nadawca oraz adresat mają dostęp do informacji, jednocześnie chronimy informację przed osobami postronnymi
- Ochrona integralności informacji – chcemy mieć pewność, że nikt nie zmienił wartości informacji
- Ochrona wysokiej dostępności informacji – chcemy mieć pewność, że informacja jest cały czas dostępna dla autoryzowanych użytkowików.

Te trzy obszary stanowią tzw. triadę bezpieczeństwa informacji, czyli pokazują jak należy myśleć w kontekście ochrony informacji. Taką definicję zobaczymy w PKN ISO 27001, czy innych regulacjach.

Przepis na Coca-Colę, szczegółowy opis patentu, wypis ze szpitala – to tylko kilka przykładów obrazujących różnie warte informacje. Można powiedzieć, że to posiadanie odpowiedniej informacji stanowi dla firmy o jej być albo nie być w biznesie. Utrata poufności informacji, np. utrata bazy klientów, może oznaczać utratę wizerunku, spadek akcji, czy w najgorszym przypadku, problemy natury formalno-prawnej.

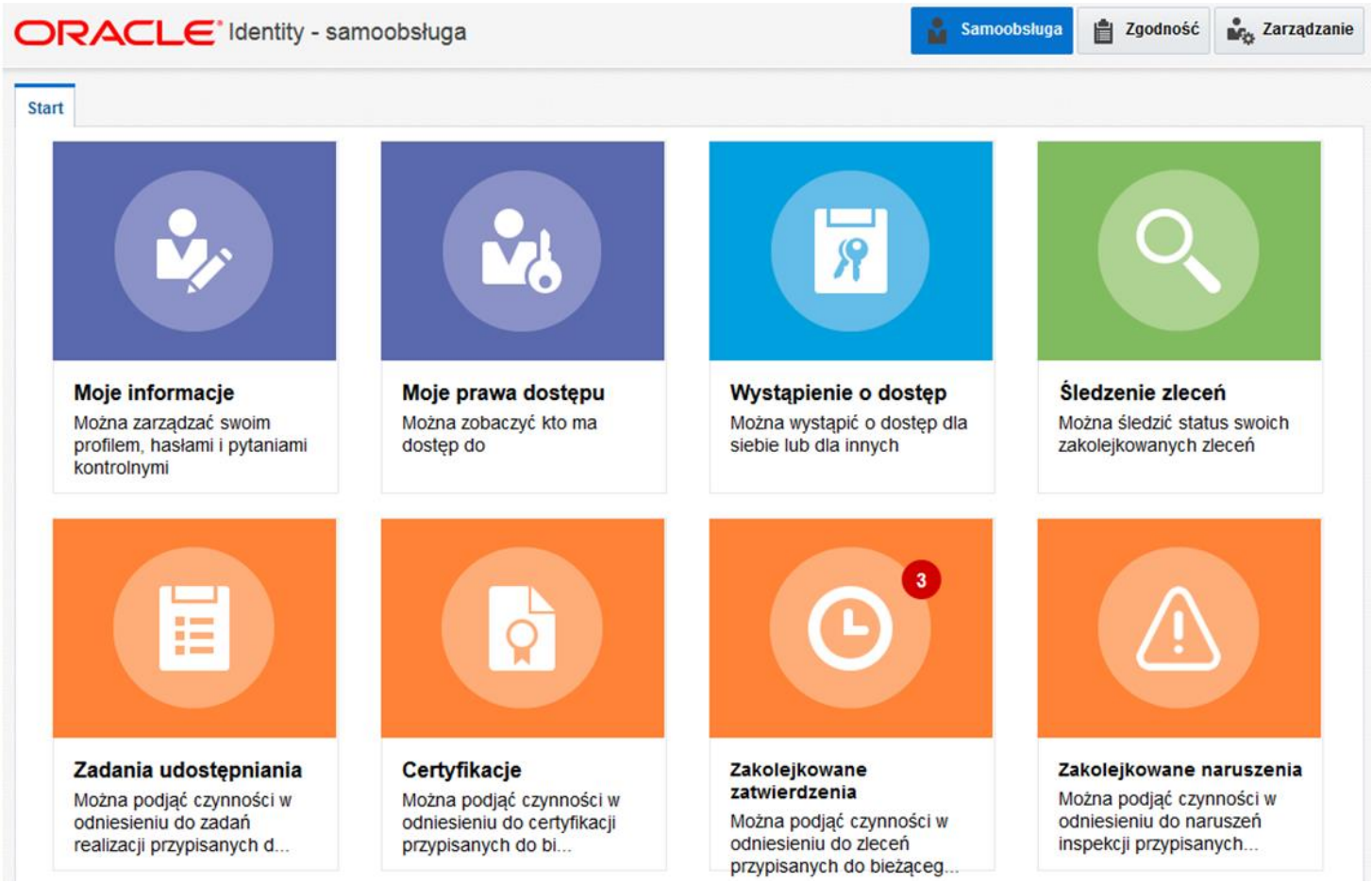
Między innymi z tych powodów firmy szukają rozwiązań za pomocą, których będą mogły kontrolować informację. W najprostszym przypadku będzie to kontrola dostępu do informacji, w bardziej złożonym, audyt oraz raportowanie.

Zauważyć można, iż w ostatnich kilku latach firmy z różnych braż chętnie wybierają zarządzaie procesowe, jako mechanizm prowadzenia przedsiębiorstwa. Oznacza to, że każdy proces ma swojego Właściciela biznesowego, odpowiedzialnego za każdy element tego procesu. Podobnie jest z informacją. Zarząd każdej firmy jest odpowiedzialny za informacje, oraz za właściwą jej ochronę. Chodzi o to, aby dane osobowe, dane finansowe czy inne wrażliwe informacje, były odpowiednio chronione. Dostęp do odpowiedniej kategorii informacji powinny mieć osoby uprawnione. Idea wydaje się prosta, ale jak kontrolować tysiące czy setki tysięcy informacji w przedsiębiorstwie?

Słów kilka o uprawnieniach

W każdym systemie informacyjnym uprawnienia są czymś, co pozwala kontrolować m.in. dostęp do informacji. Każdy Klient, niezależnie czy wewnętrzny czy zewnętrzny, posiada zestaw uprawnień pozwalający mu realizować określone zadania. **Takie zestawy uprawnień nazywane są czasami profilami lub rolami.** Wymaga się, aby w każdej chwili Pracownik mógł zweryfikować wszystkie posiadane uprawnienia i w przypadku braku wymaganych uprawnień, wnioskować o uprawnienia niezbędne mu do pracy.

Oracle IdM - Interface samoobsługi użytkownika w języku narodowym.



Rola biznesowa określa stanowisko w pracy, np. Starszy Księgowy. Osoba pełniąca takie stanowisko, posiada wszystkie niezbędne uprawnienia w systemach czy aplikacjach, które tej osobie są niezbędne do pracy. Cały proces przydzielenia wymaganych uprawnień odbywa się w specjalnym precesie workflow, w którym tworzone są określone konta w różnych technicznych zasobach (systemach, aplikacjach, aktywach). Zaleca się, aby proces akceptacji był wielostopniowyc dla systemów o większej wartości (wrażliwości), a uproszczony, wręcz automatyczny, dla systemów mniej istotnych. Przykładem może być kontrola w sytemach polegająca na weryfikacji tworzonego konta w taki sposób, w którym pierwszym weryfikującym jest bezpośredni przełożony, a następnie pracownik na stanowisku ABI (Administrator Bezpieczeństwa Informacji).

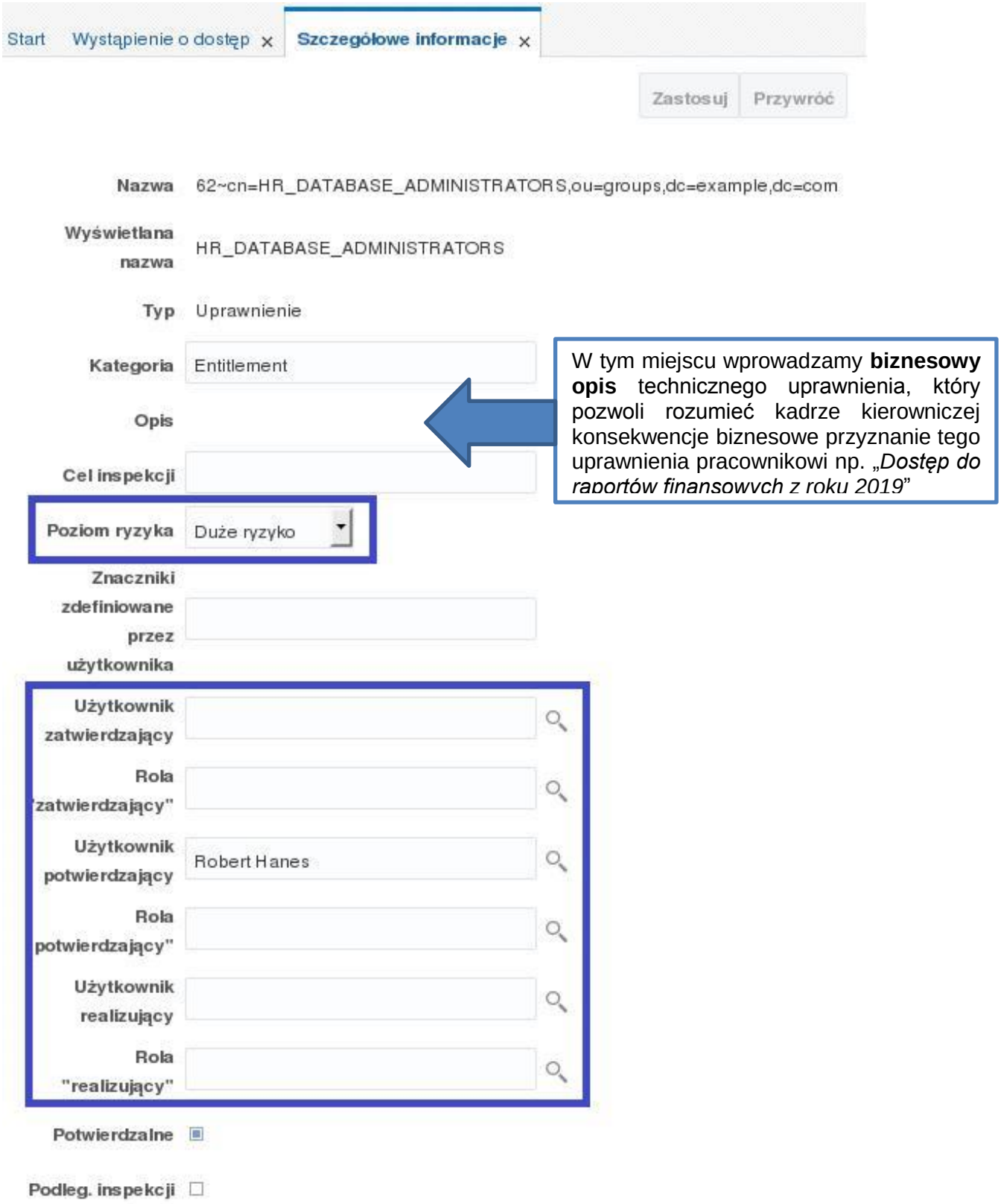
Tematyka ról jest dosyć znana, ale dopiero w ostatnich latach firmy zaczęły widzieć w zarządzaniu rolami narzędzie, które dostarczy dużą wartość biznesową. Wartość upraszczającą zarządzanie uprawnieniami, wartość pozwalającą w pełni kontrolować dostęp do informacji oraz ułatwiającą raportowanie.

Aby zilustrować problem, najlepiej posłużuć się przykładem. Najwięcej problemów przysparzają następujące, codzinne, procesy:

- Przydzielanie uprawnień dla indywidualnych użytkowników bez formalnego udokumentowania tego procesu
- Przydzielanie uprawnień dla indywidualnych użytkowników bez dokładnego zrozumienia, jakiego rodzaju uprawnienia są przydzielane („skoro uprawnienia te posiadał inny pracownik, to dla mnie też są ok")
- Sumowanie się uprawnień wraz ze zmianami na stanowiskach przez okreslonego pracownika (pracownik po kilku latach pracy posiada wiele dostępów nadmiarowych do różnych systemów i aplikacji)

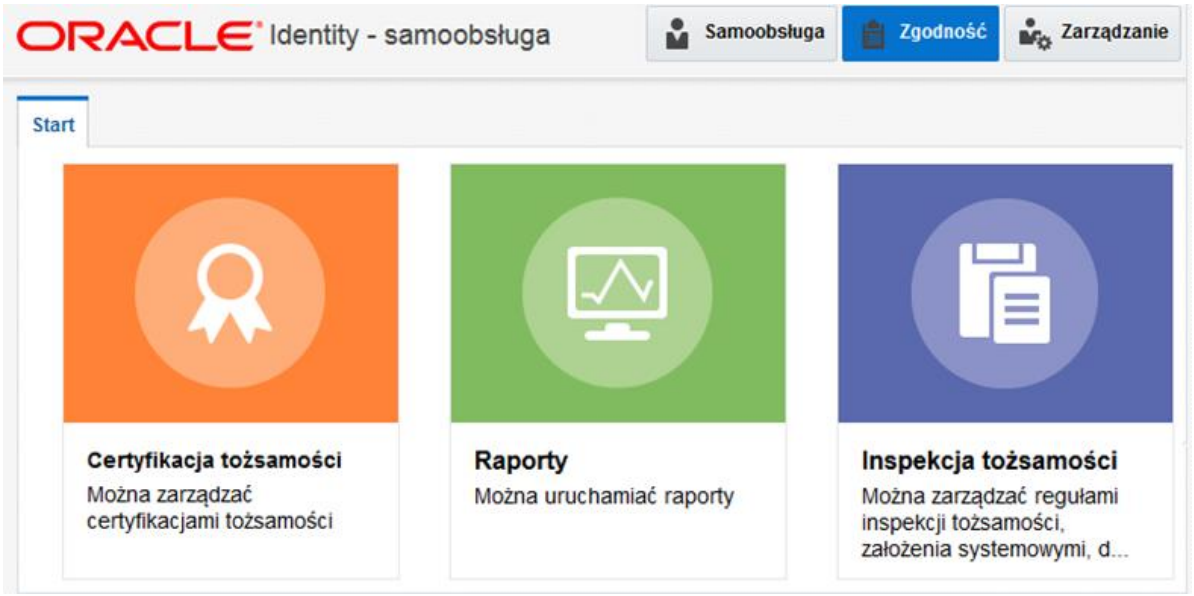
Najistotniejszym problemem jest brak zrozumienia trudnych, technicznych uprawnień, które nadawane są różnym użytkownikom. Każdy dyrektor, czy kierownik jest odpowiedzialny za uprawnienia, które posiada jego pracownik. Ponieważ złożoność systemów, z jakich firmy korzystają jest bardzo duża, a nazewnictwo uprawnień niejasne, firmy szukają rozwiązań, dzięki którym każdy kierownik będzie w pełni rozumiał, za co bierze odpowiedzialność.

Opis biznesowy trudnych, technicznych uprawnień



Warto zwrócić uwagę, że porządkowanie uprawnień należy realizować stopniowo, zaczynając od obszarów najwyższych ryzyk. Taki podział może oznaczać określony zakres systemów niezbędnych do zrealizowania najważniejszych procesów biznesowych. Często obszarem najwyższego ryzyka są dostępy określonych grup użytkowników. Należy zdawać sobie sprawę, że z praktycznego punktu widzenia, trudno jest analizować całą firmę i kontrolować wszystkie ryzyka. Takie podejście, w dłuższej perspektywie czasowej, szybko okaże się nieefektywne kosztowo.

Interface pozwalający na precyzyjną weryfikację i audyt uprawnień.



Proces certyfikacji pozwoli na osiągnięcie takich uprawnień, jakie na określonym stanowisku są wymagane. Nie więcej, nie mniej, ale dokładnie to, co jest konieczne (koncepcja zwana: least privileges). Warto wyróżnić dwa typy certyfikacji:

- Proces certyfikacji wykonywany przez właściciela informacji, tzw. Data Owner Certification,
- Proces certyfikacji wykonywany przez managera, weryfikującego uprawnienia swoich pracowników, tzw. User Entitlements Certification.

W procesie ‘Data Owner Certification’, zgodnie ze standardami bezpieczeństwa to właściciel informacji tworzy i akceptuje politykę związaną z dostępem do informacji, za które jest odpowiedzialny. Dzięki temu uzyskujemy uporządkowanie uprawnień w istniejącym środowisku, tak, aby np. późniejszy monitoring aktywności użytkowników obejmował faktycznie to, do czego użytkownicy mają mieć prawo, w ramach swojego stanowiska, a nie dużo większy obszar, powodujący, nieefektywność procesu monitoringu aktywności użytkowników.

Podsumowanie

Narzędzia nie są lekiem na wszystkie niedoskonałości związane z zarządzaniem użytkowikami i ich uprawnieniami. Większość prac związanych z uporządkowaniem tego obszaru można wykonać ręcznie. W wielu organizacjach takie procesy funkcjonują i odbiorcy biznesowi są zadowoleni. To, co jest charakterystyczne dla tak funkcjonujących firm to brak narzędzi pomiarowych, pozwalających precyzyjnie określić, jakość takiego procesu oraz jego skuteczność. Często przydzielone uprawnienia są nadmiarowe, bo nie ma narzędzie do systematycznej kontroli zakresu wykorzystywanych uprawnień. Często także zakresy uprawnień przydzielane są 'ad-hoc' czyli doraźnie, bez analizy faktycznych potrzeb, a na krótkoterminowego rozwiązania problemu. Trudno jest także, osobą odpowiedzialnym za aktywa, ocenić poziom ryzyka, a co za tym idzie konsekwencje, jakie związane są z zaakceptowaniem wybranego zakresu uprawnień.

Propozycja Euler to wykorzystanie narzędzia Oracle Identity Manager w celu uporządkowanie tego stanu, tak, aby osiągnąć spójny i powtarzalny proces zarządzania tożsamością Klienta z uwzględnieniem, jakości danych znajdujących się w systemach źródłowych.

Euler Sp. z o.o.
ul. Obrońców Tobruku 31A/130
01-494 Warszawa
e-mail: euler@euler.pl
http://www.euler.pl