

Rola działu kadr w zwiększaniu bezpieczeństwa IT

Dział personalny scala wszystkie procesy biznesowe w przedsiębiorstwie

Dział personalny jest szczególnym miejscem w strukturze każdego przedsiębiorstwa. To tutaj zbiegają się informacje o każdym pracowniku, tutaj otrzymują oni nową tożsamość związaną z zajmowanym stanowiskiem, uprawnieniami i odpowiedzialnością w firmie. To dział personalny wprowadza zmiany wynikające z awansów, ale także kadry odpowiadają na koniec za rozwiązanie stosunku pracy i odebranie wszelkich przywilejów należnych pracownikowi. Tym samym odpowiedzialność osób zajmujących się zarządzaniem zasobami ludzkimi jest ogromna i porównać ją można tylko do tej, którą ponoszą członkowie zarządu, główna księgowa i – w niektórych przedsiębiorstwach – szef ochrony bezpieczeństwa firmy.

We współczesnym świecie pracownicy działu kadr otrzymują do ręki nowoczesne narzędzia pomocne w zarządzaniu całym skomplikowanym środowiskiem, jakim jest prowadzenie spraw pracowniczych. Coraz więcej firm korzysta w tym obszarze z aplikacji zwanej potocznie SAP HR lub szerzej SAP ERP HCM (*Human Capital Management*). Są też przedsiębiorstwa korzystające z konkurencyjnych rozwiązań, takich jak Oracle PeopleSoft czy TETA HR. Aplikacje te pozwalają w wydajny sposób tworzyć konta pracowników, dokonywać zmian, prowadzić ewidencję płac czy urlopów, wreszcie zmieniać bądź rozwiązywać umowę o pracę.

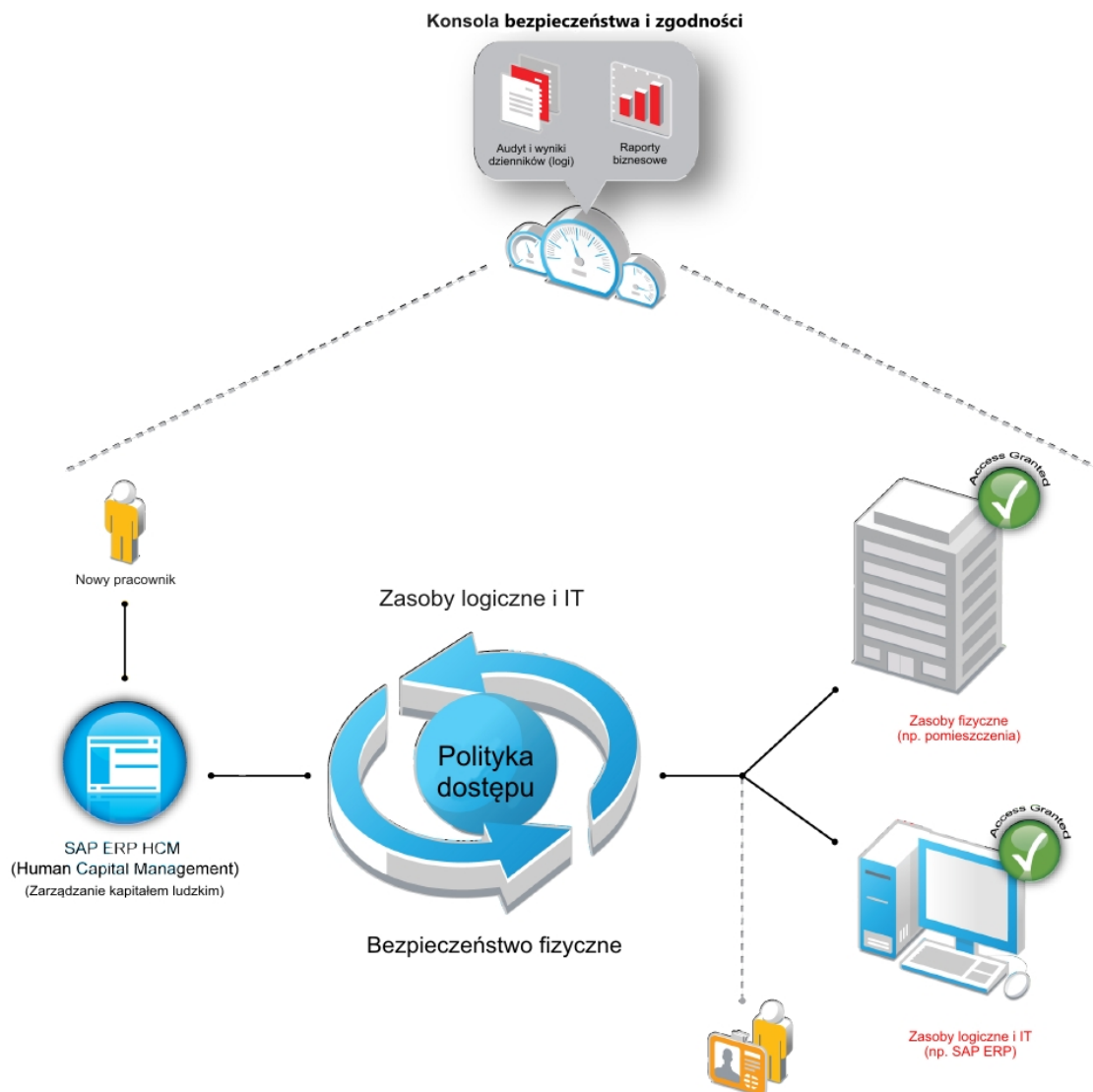
Jako element znacznie większego pakietu aplikacji biznesowych, moduł kadrowy łatwo integruje się z innymi elementami takiego rozwiązania. Jednak pełna funkcjonalność aplikacji kadrowej jest osiągnięta zazwyczaj wyłącznie wtedy, kiedy pozostałe aplikacje pochodzą od tego samego producenta. **Tymczasem w dzisiejszym świecie gospodarki elektronicznej nie zdarza się, by wszystkie systemy informatyczne, aplikacje, narzędzia, systemy dostępu do fizycznej infrastruktury przedsiębiorstwa i stanowisk pracy.** A mimo to złożoność środowiska firmy nie zwalnia pracowników kadr od odpowiedzialności za wykonywane zadania, w tym zapewnienie bądź pozbawienie dostępu do przysługujących zasobów, czy ochronę danych osobowych.

Nikt nie oczekuje od pracowników zajmujących się kadrami, by samodzielnie zapewniali integrację i dostęp pracowników do wszystkich systemów i narzędzi pracy. Jednak to właśnie z tego działu powinien wychodzić jasny przekaz do zarządu firmy i działów informatyki, ochrony, produkcji, finansów czy planowania. System kadrowy jest podstawowym źródłem informacji o pracownikach i ich umocowaniu w firmie, który musi być ściśle zintegrowany z pozostałymi elementami środowiska pracy w firmie, które z logicznego punktu widzenia są systemami pochodnymi, czerpiącymi informację o pracownikach i innych uczestnikach procesów biznesowych w firmie właśnie z aplikacji kadrowej.

Ujmując to obrazowo pracownik (w rozumieniu konta użytkownika) rodzi się, rozwija i umiera właśnie w systemie kadrowym. To z działu kadr pochodzą informacje, na podstawie których dla pracownika tworzone są konta w innych systemach (np. poczta elektroniczna czy aplikacje biznesowe), przydzielane są odpowiednie środki (np. biurko, komputer, telefon, samochód), czy wreszcie udzielane jest zezwolenie na wstęp na teren zakładu pracy czy do wydzielonych pomieszczeń szczególnego znaczenia. Do zapewnienia takiej integracji i osiągnięcia maksymalnego poziomu efektywności pracy i bezpieczeństwa firmy stosuje się nowoczesne technologie zwany potocznie „systemem zarządzania tożsamością”.

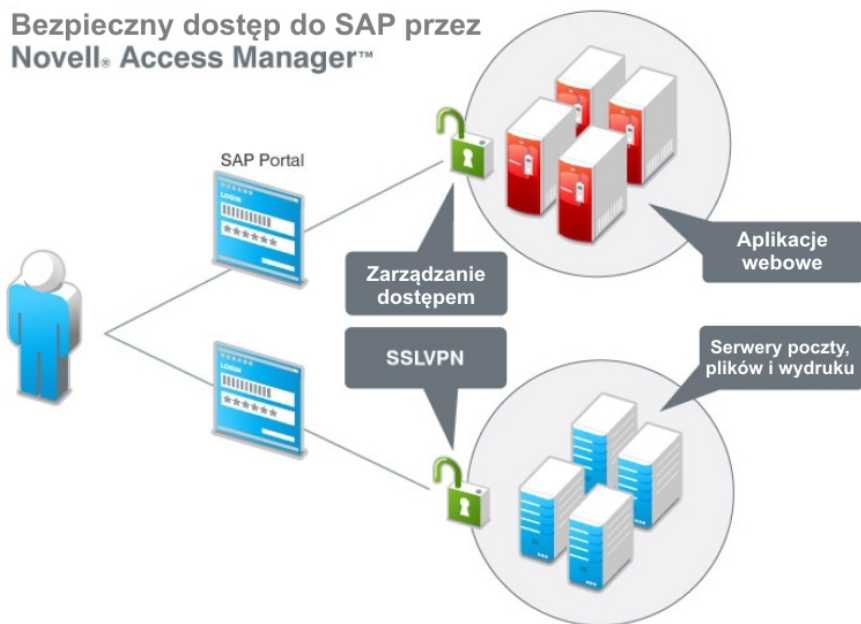
Dzięki systemowi zarządzania tożsamością zachowuje się pełną integralność danych (pracownik posiada jedno, pierwotne konto w aplikacji kadrowej, z której pobierane są dane do pozostałych systemów). W ten sposób – poprzez odpowiednie powiązania z innymi systemami teleinformatycznymi – pracownicy z jednej strony natychmiast otrzymują potrzebne im zasoby, zaś z drugiej strony mogą być skutecznie i natychmiast pozbawiani

tego dostępu w całości z chwilą rozwiązania umowy o pracę i odnotowania tego właśnie w systemie kadrowym. Dzięki temu ochronie podlegają też nie tylko środki przedsiębiorstwa, ale przede wszystkim dane krytyczne dla jego działania. Zwolnieni pracownicy nie mogą dokonać umyślnych szkód czy wykraść poufnych informacji.

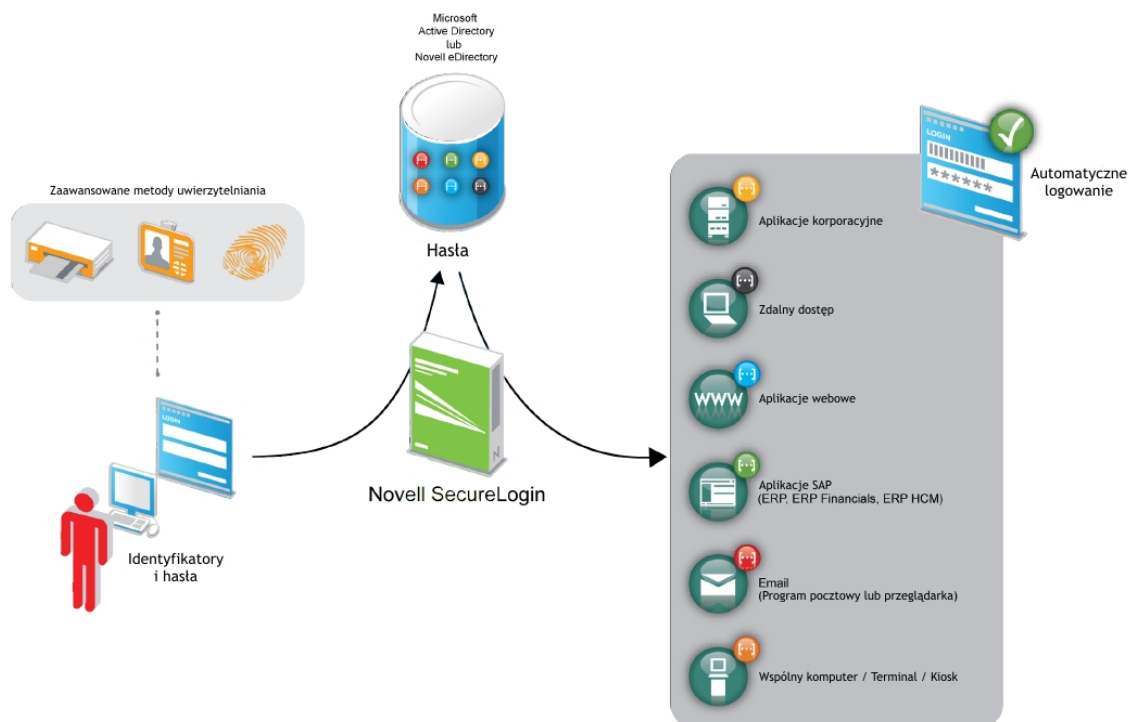


Nowoczesny system zarządzania tożsamością nie tylko chroni firmę przed zemstą zwalnianych pracowników (a jest to bolączka potwierdzona licznymi badaniami rynkowymi), ale także uniemożliwia obecnym pracownikom na dostęp wyłącznie do tych systemów, do których mają uprawnienia czy to wynikające z zajmowanego w firmie stanowiska, pełnionej roli czy udzielonych pełnomocnictw przez przełożonych. Pozwala także na uniknięcie sytuacji konfliktu interesów bądź nałożenia się uprawnień – sprzecznych z punktu widzenia interesów przedsiębiorstwa. Profesjonalnie działający system zarządzania uprawnieniami nie dopuści do sytuacji, w których na przykład osoba mająca otrzymać jakąś korzyść w firmie, sama akceptuje przyznanie sobie tych profitów. W takim systemie nawet informatycy firmy nie mają dostępu do danych, które z natury rzeczy są dostępne wyłącznie dla zarządu, księgowości czy kadr. Wszystkie procedury w firmie muszą być przestrzegane i za ich realizację oraz nadzór odpowiada właśnie system zarządzania tożsamością, który oferuje także wydajne

narzędzia do audytu i monitorowania m. in. takich zdarzeń. Co więcej, w dobie pracy zdalnej, system taki pozwala na autoryzację i przydział zasobów i kontrolę działań także tych pracowników, którzy znajdują się poza zakładem pracy.



Realizując projekty zarządzania tożsamością firmy z jednej strony wprowadzają zaawansowane mechanizmy ochrony danych i zabezpieczenia przed nieuprawnionym działaniem pracowników, zaś z drugiej strony korzystają z innego efektu takiego wdrożenia, a mianowicie ułatwienie dostępu do zasobów i środków. Jeżeli odpowiednio zdefiniujemy rolę pełnioną przez pracownika na danym stanowisku w firmie, to tym samym z chwilą utworzenia lub wprowadzenia zmian w koncie danej osoby, możemy natychmiast i w zupełnie automatyczny sposób tworzyć konto użytkownika w systemie pocztowym i innych aplikacjach, czy systemach dostępowych. A jeżeli mamy jedno konto pracownika, to tym samym możemy uprościć proces autoryzacji. Tym samym jedno hasło, czy hasło powiązane z kartą dostępową, pozwala na dostęp pracownika do wszystkich przydzielonych mu zasobów. Koniec z zapamiętywaniem dziesiątek odrębnych haseł! Nawet jeżeli ze względów bezpieczeństwa nadal niektóre systemy wymagają osobnych metod logowania, to system zarządzania tożsamością, który z natury oferuje najsilniejsze mechanizmy uwierzytelniania i autoryzacji, zadba o przejrzysty dla użytkownika proces logowania. Inaczej mówiąc pracownik loguje się raz i ma dostęp do właściwych zasobów, ale tylko po wcześniejszej weryfikacji w systemie zarządzania tożsamością.



Podsumowanie – korzyści biznesowe

W nowoczesnym przedsiębiorstwie rola działu kadr wykracza daleko poza tradycyjne funkcje. Oczywiście nie oznacza to, że pracownicy kadr muszą mieć wiedzę informatyczną. Jednak każdy pracownik odpowiada za procesy biznesowe i wpływa na wartość przedsiębiorstwa. Nie inaczej jest z kadrami, których pracownicy mają chyba największy wpływ na produktywność i drożność procesów i procedur wewnętrznych w firmie. Poprzez wymuszenie integracji aplikacji kadrowej z pozostałymi systemami teleinformatycznymi Kadry w naturalny sposób mogą w bezpieczny i odpowiedzialny sposób przyjąć na siebie współodpowiedzialność za działanie przedsiębiorstwa.

Poniżej przedstawiono najważniejsze korzyści z wdrożenia systemu zarządzania tożsamością:

- Automatyczne przydzielanie lub odbieranie dostępu do fizycznych i logicznych zasobów firmy.
- Kompletnie i łatwe monitorowanie zdarzeń i tworzenie raportów.
- Zapewnienie zdalnym pracownikom dostępu z wykorzystaniem kart/tokenów.
- Blokowanie stanowisk pracy chroniące przed nieautoryzowanym dostępem.
- Wykorzystanie złożonych i zaawansowanych metod weryfikacji tożsamości.
- Możliwość tymczasowego przydzielania zasobów po weryfikacji tożsamości w kadrach.
- Konsekwentne wymuszenie stosowania ustalonych procedur biznesowych w firmie.
- Zweryfikowanie i opisanie uprawnień użytkowników, określenie ich ról i przywilejów w określonych przedziałach czasowych.
- Wymuszenie rozdzielania obowiązków, by nie dochodziło do konfliktu interesu lub naruszenia procedur.
- Automatyczny przydział lub odebranie uprawnień na podstawie procedur biznesowych.
- Obniżenie złożoności i uproszczenie zarządzania zasobami teleinformatycznymi.
- Możliwość przeniesienia odpowiedzialności na właścicieli projektów biznesowych w celu weryfikacji lub osiągnięcia elastyczności działania firmy.
- Możliwość wychwycenia nakładających się zależności lub dublującej się odpowiedzialności między pracownikami lub działami w przedsiębiorstwie.

- Zgodność ze standardami branżowymi, regulacjami krajowymi i międzynarodowymi.
- Wymuszenie konsekwentnego stosowania procedur na podstawie reguł zdefiniowanych przez SAP lub innych dostawców, bądź własnych procedur.
- Zabezpieczenie wszystkich zasobów (także webowych) w sposób automatyczny i bez konieczności modyfikacji istniejących systemów i aplikacji.
- Zapewnienie pracownikom jednakowych metod autoryzacji bez względu na miejsce, w którym się znajdują.
- Dostęp do aplikacji SAP i innych zasobów biznesowych z wykorzystaniem autoryzacji jednokrotnego logowania (*single sign-on*).
- Przydzielenie osobom spoza firmy (partnerom, dostawcom, osobom na kontrakcie) w pełni kontrolowanego dostępu do wybranych zasobów firmy.
- Uniknięcie konieczności zapamiętywania osobnych haseł do wielu aplikacji i zasobów, co m.in. pozwala na odciążenie działu IT (*help desk*).
- Zwiększenie ochrony krytycznych zasobów, w tym danych znajdujących się w systemach SAP.

W celu osiągnięcia tych wszystkich korzyści zapraszamy do kontaktu z firmą Novell, liderem na rynku producentów systemów zarządzania tożsamością na świecie:

Novell Sp. z o.o.
ul. Postępu 21
02-676 Warszawa
infolinia: 0-800 226685
infolinia@novell.pl
www.novell.pl