Případová studie nasazení Identity Management (IDM)

Jedno heslo – Jedna role

Cíl projektu: Efektivní správa přístupových oprávnění uživatelů – napojením na HR systém klienta se změny (přidání, odebrání či změna účtu) v aplikacích budou provádět automaticky s nástupem či odchodem zaměstnance, popřípadě změnou v údajích o něm (změna příjmení, povýšení apod.). Hlavní důraz se přitom bude klást především na rychlost, správnost a dohledatelnost prováděných změn. To mimo jiné předpokládá i výraznou redukci stávajícího počtu uživatelských rolí, díky kterým bude možné řídit oprávnění uživatelů v podnikových aplikacích.

PŘÍPADOVÁ STUDIE

Technologie IDM

- **Microsoft Active Directory** (Windows domain) – řídí bezpečnost pracovních stanic.
- **Oracle Identity Manager** – centrální správa identit a rolí, integrována s HR systémem, řídí účty a oprávnění v podnikových aplikacích VZP ČR.
- **Oracle Enterprise Single Sign On** – komponenta zajišťující automatické vyplnění jména a hesla pro technologicky různorodé podnikové aplikace.
- **Oracle Virtual Directory** – komponenta poskytující LDAP rozhraní.
- **Externí, konsolidované úložiště aplikačních rolí** – na míru vytvořené databázové řešení s LDAP rozhraním pro podnikové aplikace.

POSKYTNUTÉ SLUŽBY

Další cíle projektu

- **Uživatelský komfort (SSO)** – zaměstnanec klienta bude pro svoji běžnou práci potřebovat znát pouze jediné heslo. Všechna ostatní aplikační hesla již nebude znát a platforma IDM je bude automaticky spravovat a vyplňovat při přihlašování do podnikové aplikace.
- **Jednotně definovaná úroveň zabezpečení** – zákazník bude mít možnost definovat politiku hesel napříč spektrem podnikových aplikací dle aktuálních bezpečnostních potřeb; díky SSO se tyto změny nijak nepromítnou do pracovní rutiny zaměstnanců.

Přínosy

- Omezení rizika „propůjčování“ cizí identity
- Maximalizován uživatelský komfort díky Single Sign-On, tj. uživatel je automaticky přihlašován do aplikací
- Zamezení existence „nekontrolovaných“ aplikačních účtů
- Efektivní řízení oprávnění díky vytvořeným celopodnikovým rolím (pouze desítky rolí pro 5000 zaměstnanců)
- Unifikované procesy řízení identit a oprávnění napříč všemi územními pracovišti společnosti
- Správnost a aktuálnost dat je zajištěna prostřednictvím rychlé propagaci změn do všech IT systémů z autoritativního zdroje – personálního systému
- Redukce mnoha úložišť aplikačních rolí – do jednoho společného konsolidovaného úložiště, který poskytuje standardizované rozhraní LDAP

Výhody

- Automatické přihlašování do všech zpřístupněných aplikací na základě jediného ověření

GEM System a. s. | Štětkova 1638/18, 140 00 Praha 4 – Nusle | sales@gemsystem.cz | www.gemsystem.cz

Integrované systémy

- Microsoft Active Directory
- Microsoft Exchange 2010
- Microsoft SharePoint
- Aplikace realizované na míru (Oracle Forms, Oracle DB)
- SAP R/3
- LMS (MS SQL)
- Cisco VPN
- Vema HR systém

VŠEOBECNÁ ZDRAVOTNÍ POJIŠŤOVNA ČESKÉ REPUBLIKY

VZP ČR byla založena v roce 1992 a dlouhodobě patří k základním pilířům systému zdravotnictví v ČR. S více než 6,2 miliony klientů je největší zdravotní pojišťovnou v České republice.

Charakteristika VZP ČR v číslech

- 5 000 zaměstnanců,
- 1 200 organizačních útvarů,
- desítky podnikových systémů (AD, Exchange, Oracle Forms, Oracle DB, SAP R/3, MS SQL),
- rozsáhlá síť poboček,
- nejširší síť smluvních zdravotních zařízení.

Hewlett Packard Enterprise

Hlavní integrátor projektu

Přední dodavatel technologií pro tiskové řešení, osobní výpočetní techniku, software, služby a IT infrastrukturu.

ORACLE®

Světový dodavatel integrovaného podnikového software a hardwarových systémů.

- Zvýšené bezpečnostní standardy klienta
- Jednoznačné přidělení uživatelských kompetencí

Realizace projektu

Realizace projektu, vedená hlavním integrátorem společností Hewlett-Packard, spočívala jak v technologické, tak procesní rovině. V prvním případě se jednalo o implementaci a integraci jednotlivých IT systémů, v tom druhém pak o redesign příslušných podnikových agend. Vzhledem k faktu, že zákazník dlouhodobě využíval produkty společnosti Oracle, integrátor projektu Hewlett-Packard se rozhodl využít IDM řešení právě této značky. Navíc široká nabídka Oracle v segmentu IDM splňovala všechny předpoklady pro vznik takového řešení, které by beze zbytku pokrylo potřeby klienta.

Klíčovou součástí celého řešení je Oracle Identity Manager. Ten se po nasazení do prostředí zákazníka stal jakýmsi „centrálním mozkem", který ovládá veškeré uživatelské účty a oprávnění v podnikových aplikacích, a to včetně Oracle eSSO. Je propojen se zákazníkovým personálním systémem, kterému byla v celém IDM řešení přidělena role autoritativního prvku. Díky tomu se veškeré změny týkající se údajů o zaměstnancích automaticky adekvátně promítnou i do údajů o jednotlivých účtech a uživatelských oprávněních. Personální systém tak nyní má jako jediný jednoznačnou odpovědnost za stav podnikových aplikací z pohledu uživatelů a jejich oprávnění, což správu a řízení účtů výrazně zjednodušuje a zrychluje.

Za tímto účelem bylo pro potřeby personálního oddělení nutné redefinovat tzv. podnikové role. Nyní mohou personalisté jednoduše přímo specifikovat různá oprávnění pro jednotlivé pozice v organizační struktuře klienta. To mimo jiné odstranilo problém s kumulováním více oprávnění, k němuž dříve docházelo z důvodu postupného působení zaměstnance na několika pracovních pozicích.

Zejména se jedná o efektivní správu identit a rolí pro více než pět tisíc zaměstnanců postavené na automatizované propagaci změn z personálního systému do dalších IT systémů zákazníka. Tím se rapidně redukoval objem manuální administrace a pokryl se kompletní životní cyklus identity (například nástup do firmy, změna pozice, odchod z firmy apod.).

Z uživatelského hlediska je hlavní výhodou nového IDM řešení jednoznačně automatické přihlašovaní do všech zpřístupněných aplikací na základě jediného ověření při loginu do systému Windows. Zaměstnanec si tak nemusí pamatovat více hesel a snadněji může přecházet mezi souběžně spuštěnými podnikovými aplikacemi.

IDM projekt také výrazně zvýšil bezpečnostní standardy klienta. Veškeré aplikační účty jsou napárovány na konkrétní zaměstnance, tudíž činnost provedená pod daným účtem má rychle a jasně identifikovatelnou odpovědnost. Provázání IDM na personální systém firmy také znamená jednoznačné přidělení uživatelských kompetencí a jakékoli změny v IT systémech souvisejících s účty a jejich oprávněními jsou zpětně dohledatelné.