JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Katedra matematiky a informatiky

Studijní program: B6209 Systémové inženýrství a informatika

Studijní obor: Ekonomická informatika

Identity a jejich správa v podnikovém prostředí

Bakalářská práce

Vedoucí bakalářské práce: Mgr. Radim Remeš

Autor: Petr Klíma

2013

Prohlášení Prohlašuji, že v souladu s § 47 zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské/-diplomové práce, a to - v nezkrácené podobě/v úpravě vzniklé vypuštěním vyznačených částí archivovaných Ekonomickou fakultou - elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

2013-02-19

Datum Podpis

Poděkování chtěl bych se poděkovat dvěma Jiřím kteří mě vedlou světem výpočetní techniky. Jiřímu Zatloukalovi za uvedení do principů počítačových sítí a síťových technologií - z našich diskusí čerpám dodnes. A také Jiřímu Gabrielovi který ví "jak se v CPU tahá za drát". Sice tahám za kratší konec, ale každý náš počítačový brainstorming je školou sám osobě.

Obsah

Seznam obrázků

Seznam tabulek

JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH
Fakulta ekonomická
Akademický rok: **2011/2012**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr KLÍMA**
Osobní číslo:	**E10359**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Ekonomická informatika**
Název tématu:	**Identity a jejich správa v podnikovém prostředí**
Zadávající katedra:	**Katedra aplikované matematiky a informatiky**

Zásady pro vypracování:

Cílem bakalářské práce je porovnat dostupné metodiky správy identit a řízení zdrojů ve firmách, vybrat a navrhnout implementaci zvolené metodiky v konkrétní firmě.

Metodický postup:

1. Studium odborné literatury.
2. Obecný popis metodik správy identit a řízení zdrojů.
3. Teoretický popis konkrétních dostupných metodik pro správu identit.
4. Porovnání a analýza vybraných metodik, zhodnocení jejich použitelnosti pro nasazení v reálném prostředí.
5. Popis implementace metodiky správy identit ve zvolené firmě.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40-50 stran**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

1. **BERTINO Elisa a Kenji TAKAHASHI.** *Identity Management: Concepts, Technologies, and Systems.* **Norwood (Massachusetts): Artech House, 2011. 196 s. ISBN 978-1608070398.**
2. **HOLME Dan.** *Windows Administration Resource Kit: Productivity Solutions for IT Professionals.* **Redmont: Microsoft, 2008. 752 s. ISBN 978-0-7356-2431-3.**
3. **KRÁL, Jaroslav.** *Informační systémy: specifikace, realizace a provoz.* **1. vyd. Veletiny: Science, 1998. 358 s. ISBN 80-86083-00-4.**
4. **POHLMAN, Marlin, B.** *Oracle Identity Management: Governance, Risk, and Compliance Architecture.* **3rd ed. Boca Raton (Florida): CRC Press, 2008. 552 s. ISBN 978-14-200-7247-1.**
5. **WILLIAMSON, Graham, David YIP, Ilan SHARONI a Kent SPAULDING.** *Identity Management: A Primer.* **Lewisville (Texas): Mc Press, 2009. 200 s. ISBN 978-1583470930.**

Vedoucí bakalářské práce: **Mgr. Radim Remeš**
Katedra aplikované matematiky a informatiky

Datum zadání bakalářské práce: **19. ledna 2012**
Termín odevzdání bakalářské práce: **12. dubna 2013**

doc. Ing. Ladislav Rolínek, Ph.D.
děkan

L.S.

prof. RNDr. Pavel Tlustý, CSc.
vedoucí katedry

V Českých Budějovicích dne 29. března 2012

ABSTRACT

Cíl práce Cíl práce je porovnat způsoby používání identit ve společnostech. Porovnat rozdíly v přístupu a složitosti jejich správy v závislosti na velikosti společnosti a počtu uživatelů a/nebo aplikací. Posoudit vhodnost jednotlivých přístupů ke správě identit ve vybrané společnosti střední velikosti. Zdůraznit klady, zápory a na závěr provést výběr vhodného přístupu. Popsat jednotlivé kroky při uvádění vybraného přístupu ke správě identit do činnosti.

ENGLISH TITLE Identities and identity management in a midsize company.

VEDOUCÍ PRÁCE REMEŠ Radim, Mgr.

ZÁSADY PRO VYPRACOVÁNÍ Cílem bakalářské práce je porovnání dostupných způsobů pro správu identit, výběr vhodného typu a příprava implementace.

Kapitola 1

Úvod

V posledních 20 letech došlo k obrovskému rozmachu využívání informačních technologií (dále jen IT). Především v západní civilizaci pronikly téměř do všech oblastí lidské činnosti. Oblast IT byla dřív doménou velkých firem a několika málo nadšenců, to zejména z důvodů náročnosti – finanční i odborné – pořizování IT prostředků i udržování v efektivním chodu. Nyní se IT využívá v podnicích všech velikostí i domácnostech. Tyto změny si vynutily od dodavatelů IT na všech úrovních veliké změny v přístupu k užívání, uživatelům, správě a údržbě těchto prostředků, jejich uživatelské přívětivosti a odolnosti vůči nestandardnímu, neodbornému využívání, případně i pokusům o zneužití.

S penetrací IT do fungování společnosti roste důraz na zabezpečení důvěrnosti a opravdovosti (autenticity) informací a potvrzení (authorizaci) přístupu k prostředkům. Jednou z mnoha opatření které jsou použity v celém souboru metod pro zabezpečení fungování IT prostředků je identifikace uživatelů nebo entit užívajících tyto prostředky.

1.1 Cíl práce

Správa identit (**Id**entity **M**anagement – dále jen IdM) je jedna z částí správy IT prostředků která může rozhodnout o úspěšnosti vnímání nasazení IT ve společnosti, a to jak ze strany uživatelů, tak i vedení společnosti, případně vlastníků. Vedení organizace klade důraz na efektivní fungování IT při zachování pro podnik důležitých funkcí – bezpečnost, autentičnost, auditovatelnost – a to v míře pro organizaci potřebné. Uživatelé silně vnímají komfort nebo naopak překážky které jim používání identit přináší a ocení pokud se jim příliš nepřekáží v práci.

Výběr způsobu jak v organizaci přistoupit k IdM může výrazně přispět k efektivitě užívání IT ve společnosti. Tato práce si klade za cíl utřídit informace o možnostech IdM, nastínit jaké jsou možné výchozí stavy a pokusit se předestřít možnosti nasazení v organizacích s různým výchozím prostředím a různými požadavky.

Kapitola 2

Základní pojmy

V této kapitole se seznámíme se základními pojmy z oblasti IdM. Vysvětlení některých pojmů je důležité z důvodu správného pochopení principů IdM.

2.1 Entita

Entita označuje všeobecný objekt, nezávisle na jeho existenci, který lze považovat za základní jednotku systému. Z pohledu IdM je asi nejvýstižnější definice vycházející z významu identity:

> *Entita je reprezentována jednou nebo několika identitami podle daného kontextu.* (Jøsang, Pope, 2005)

Tato definice potvrzuje, že entita a identita nejsou totožné a mohou označovat objekty bez omezení na osoby. Z pohledu IdM je tato definice dostačující, neboť umožní do správy identit zahrnout nejen osoby, ale i ostatní zdroje – např. výrobní zařízení, automobily, budovy.

2.2 Identita

Jako slovo má identita mnoho významů. V matematice jich má hned několik, další významy můžeme najít v psychologii, sociologii, filozofii a marketingu. Lze ji požít pro popis shodnosti nebo stejnosti. Pro použití v IdM je však patrně nejvýstižnější totožnost. V literatuře můžeme najít různé definice identity. Velmi obecně pojatá, avšak omezená na osoby je tato definice:

> *Identita jednotlivce může zahrnovat mnoho dílčích identit, z nichž každá představuje osobu v určitém kontextu nebo roli. To znamená, že neexistuje* ***ta Totožnost****, ale sada totožností, jež jsou podmnožinami hodnot komplexní identity, kde komplexní identita je množinou všech hodnot atributů všech totožností osoby.* (Pfitzmann, Hansen, 2010)

Jiná definice je úspornější, ale stále zaměřená pouze na osoby:

> *Identita souvisí se sadou přístupů, mechanismů a procesů týkajících se zveřejňování informací o osobě a používání těchto informací.* (Nabeth, 2006)

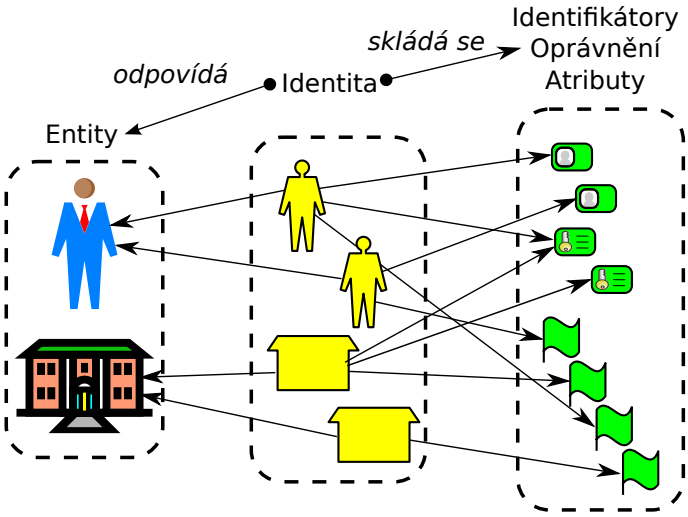
Identita se však může týkat i jiných subjektů než osob. Proto vznikly další možné definice:

> *Identita je jednoznačné určení jedinečného subjektu.* (Bishop, 2003)

nebo

> *Identita je informace o entitě, která je dostatečná k identifikování v daném kontextu.* (ITU-T, 2009)

Definice organizace ITU (International Telecomunication Union) se mi zdá nejpříhodnější, protože je přesná, přesto umožňuje aplikaci na široké spektrum subjeků a úhlů pohledu na ně (kontext).



Obrázek 2.1: Koncept identit (Jøsang, Pope, 2005)

2.3 Atribut

Atributy jsou z pohledu IdM informace(data), související nebo popisující identitu. Každá identita obsahuje tato data v několika druzích. Jsou to především (ITU-T, 2009):

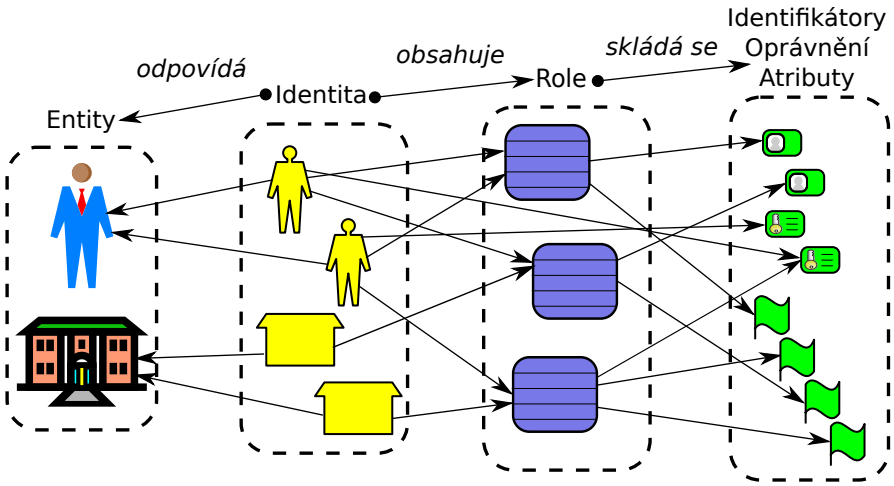
Identifikátory identifikují subjekt v daném čase a místě, např. osobní číslo, email ...

Oprávnění umožňují potvrdit, že subjekt je entita, za kterou se vydává – např. heslo

Atributy dodatečná data charakterizující entitu – např. titul, prac. zařazení, místo práce, práva do inf. systému ...

2.4 Role

V některých případech je možné/výhodné atributy seskupovat do sad které je poté možno aplikovat na identity. Tyto sady se označují jako role. Jejich význam je především v možnosti na jednom místě soustředit atributy společné několika identitám – např. zaměstnanci s pracovním zařazením „účetní“ budou mít společné atributy popisující jejich prac. zařazení a přístupová práva. (Justus, 2010)



Obrázek 2.2: Koncept rolí (Jøsang, Pope, 2005)

2.5 Provisioning

Znamená – poskytnutí služby uživateli včetně veškerého vybavení, instalací a nutného nastavení. Konkrétně lze provisioning popsat na příkladu počítače, který bude mít před předáním uživateli vytvořený uživatelský účet, nastavený e-mail a nainstalovaný potřebný software.

Využitím automatického provisioningu lze velmi ulehčit IT oddělení, které se nemusí zabývat tímto často se opakujícím, v podstatě rutinním úkonem.

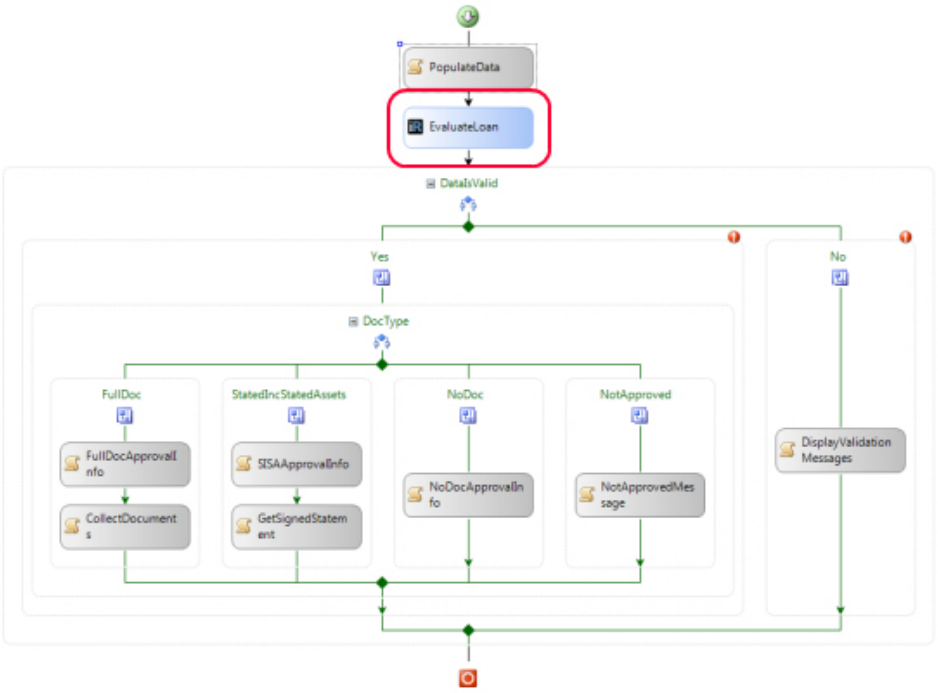
2.6 Workflow

Workflow popisuje činnost, aktivitu nebo process rozepsaný do menších částí, postupných kroků a úklolů. V IdM je používán ve dvou typech úloh.

Žádost o změnu přístupu kdy workflow popisuje process jak lze získat změnu přístupových práv a to včetně povolování od nadřízených nebo správců zdrojů a reakcí na možné stavy žádosti.

Nastavení změn kdy workflow popisuje jak nastavit změny, buď automaticky, nebo v součinnosti s obsluhou systému a provádí definované reakce na stavy při provádění těchto změn.

Z pohledu IdM workflow, stejně jako provisioning, ulehčí IT oddělení vykonávání opakujících se rutinních úkolů a umožní, aby se věnovala primárně úkolům, které vyžadují lidský zásah.



Obrázek 2.3: Příklad workflow (Emden, 2011)

2.7 Korelace a rekonciliace

Vzhledem k tomu, že IdM může agregovat identity z/do různých zdrojů, potřebuje mechanismy kterými dokáže identifikovat stejné entity v různých identitách pocházejících z různých systémů. A to ať se funkce IdM provádějí ručně nebo jsou automatizovány.

Používají se k tomu dva mechanismy:

korelace identit popisuje – za pomoci korelačních pravidel – jakým způsobem identifikovat identity z různých zdrojů na entity. Je potřeba zejména proto, že v různých systémech může mít identita jinou sadu atributů. V IdMS je většinou plně automatická.

rekonciliace identit popisuje jakým způsobem řešit konflikty při identifikaci identit. Může se, podle nastavených pravidel, pokusit provést identifikaci automaticky, iniciuje workflow, kdy je na nesoulad upozorněna obsluha nebo je spuštěn jiný proces – např. blokace systému z důvodu možného porušení bezpečnostních pravidel.

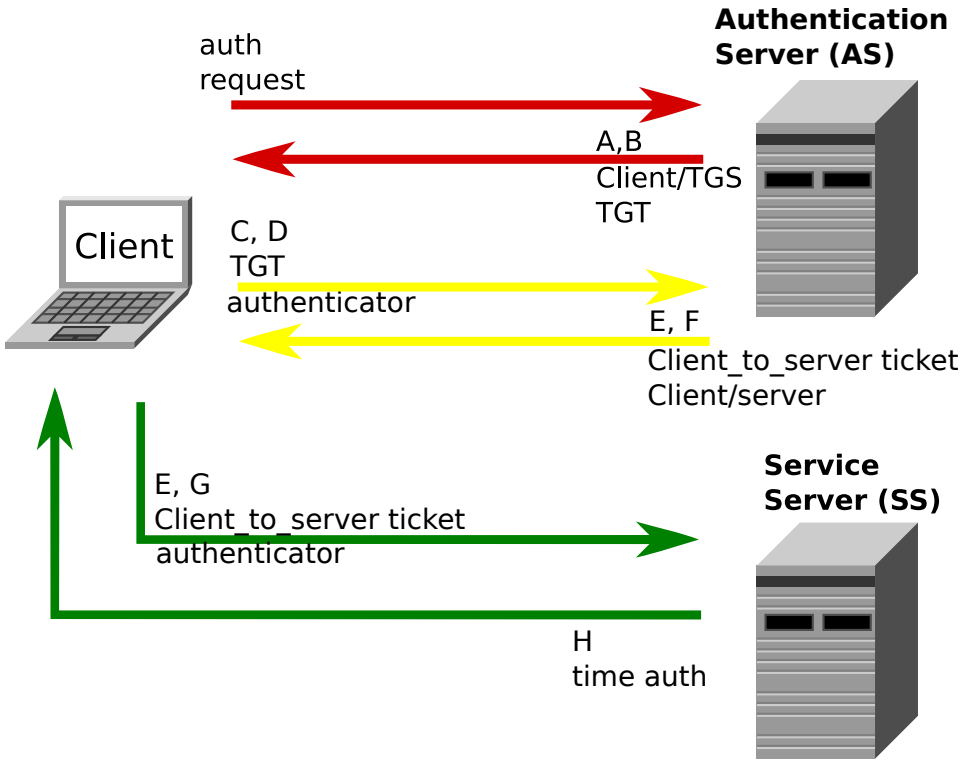
Korelace a rekociliace mají v IdM nezastupitelnou roli a to ať v provozním smyslu kdy ulehčují práci IT oddělení, nebo z bezpečnostního pohledu, kdy napravují či upozorňují na chybu, nebo dokonce záměrnou manipulaci s identitou.

2.8 SSO

SSO (**S**ingle **S**ign-**On**) je obecný název pro službu, která umožní minimalizovat počet autentizací a tím umožnit používat silný mechanismus autentizace, který by při častém použití byl uživatelsky nepřívětivý.

Takováto služba akceptuje autentizaci od uživatele a poté ji prezentuje aplikacím a systémům, které jsou zapojené do SSO, uživatel už se nemusí přihlašovat. Výhoda pro uživatele je zmíněna v předchozím odstavci, nevýhodou je, že útočník který získá tuto jednu autorizaci, má okamžitě přístup ke všem zdrojům napadeného účtu.

Nejrozšířenější SSO je pravděpodobně Kerberos který pracuje na principu „ticketu“ který uživatel získá při přihlášení a poté ho prezentuje poskytovateli služby. Princip je ukázán na následujícím obrázku.



Obrázek 2.4: Kerberos (Snock, 2011)

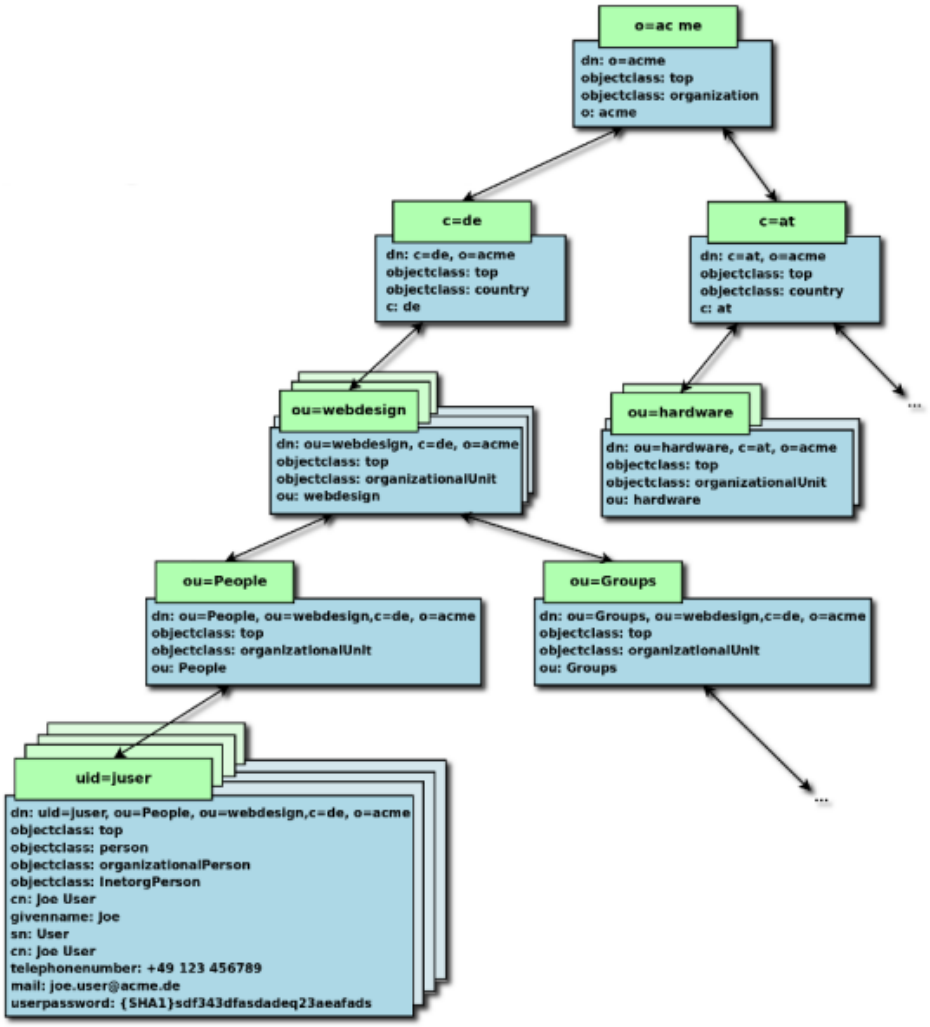
2.9 Adresářová služba

Adresářová služba je obecné úložiště identit, kde jsou identity uloženy včetně všech atributů. Takovéto úložiště je zpřístupněno pro lokální i vzdálené dotazy na identity nebo jejich ověření.

Nejstarší systémy používaly distribuování souborů s identitami na všechny stroje, kterých se adresářová služba týkala. Jako příklad lze použít NIS nebo NIS+ společnosti SUN Microsystems.

Jako základ nejrozšířenějších současných systémů je norma X.500 (norma CCITT – dnes ITU-T) (CCIT, 1988) nebo novější verze ISO/IEC 9594-1 (ISO, 2011). Adresářová služba vycházející z X.500 je koncipována jako globální, komplexní služba a právě této složitosti se připisuje nedostatek implementací a nasazení v reálném provozu.

Novější systémy vycházejí z X.500, ale drží se zásady „dostatečně dobrého“ (Principle of good enough), kdy si z X.500 vzaly principy a implementovaly je tak aby stačily požadovanému účelu. Nejrozšířenější z těchto systémů je LDAP (Lightweight Directory Access Protocol) popsaný v RFC 4511 (Sermersheim, 2006) a jeho rozšířená implementace firmy Microsoft s názvem Active Directory.



Obrázek 2.5: Příklad struktury LDAP (Aphroland, 2013)

2.10 IdM

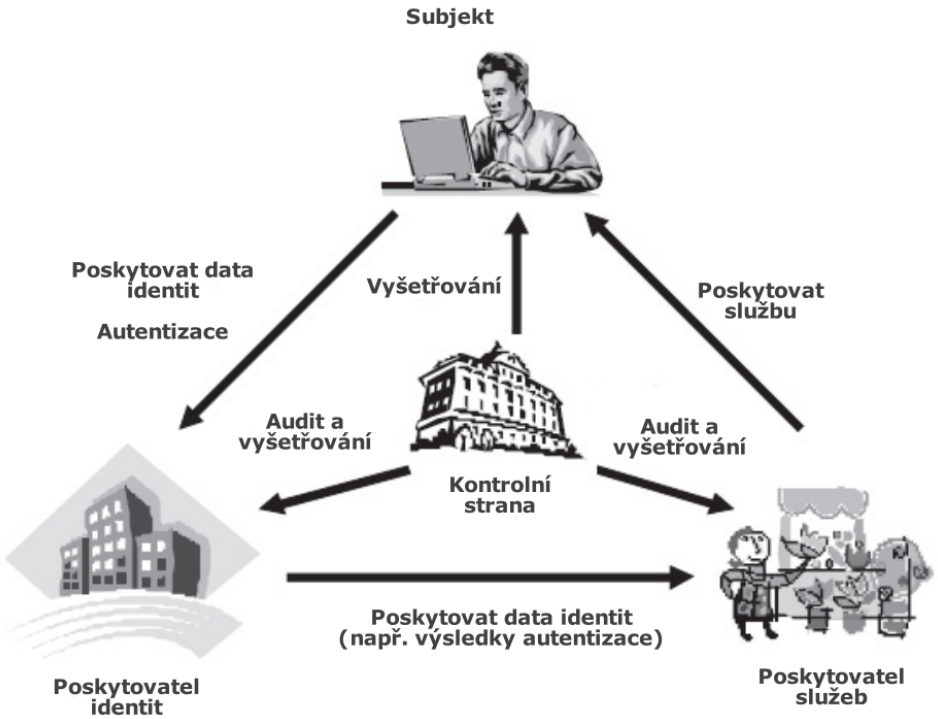
Správa identit pokrývá je velice široké pole nakládání s identitami. Správu identit (IdM) se pokusilo definovat mnoho dokumentů, které se problematiky týkají. Několik výstižných definic:

> *Identity management je strukturovaná tvorba, zachycení, syntaktický výraz, skladování, označování, údržba, vyhledávání, využívání a zneškodňování identit pomocí různých technických, provozních a právních systémů a postupů.* (ITU-T, 2009)

> *Identity management se snaží o zachování integrity identit během životního cyklu za účelem zpřístupnit identity a jejich dostupná data službám zabezpečeným a chráněným způsobem.* (Bertino, Takahashi, 2011)

> *Podnikový identity management je množina business procesů a podpůrné infrastruktury, která poskytuje řízení přístupů k systému a zdrojům na základě identit a v souladu se zavedenými politikami.* (Harrop, 2009)

Vztahy mezi účastníky IdM nejlépe vystihuje toto schéma od International Telecomunication Unie



Obrázek 2.6: Účastníci IdM (ITU-T, 2009)

Kapitola 3

Výchozí stav

Potřebu správy identit si můžeme ilustrovat na menší úspěšné společnosti která se svým růstem dostává z pohledu IT oddělení a správy IT prostředků do segmentu střední společnosti. Tím se pro nutně vzniklé firemní IT otvírá několik oblastí, ve kterých bude dříve nebo později donuceno okolnostmi vyvinout nástroje, postupy nebo pravidla fungování.

Malé společnosti začínají obvykle s několika málo počítači, její IT infrastruktura většinou vzniká živelně. Podobná situace je i s programovým vybavením, aplikace jsou pořizovány podle potřeby, většinou bez systematického přístupu.

HLAVNÍ ZNAKY

- Přístup k aplikacím a IT prostředkům je poskytován podle potřeby (někdy ”všechno všem”)
- Často jsou přístupy sdíleny
- Hesla bývají známá více uživatelům, nemění se
- IT podpora – stačí poučený uživatel

S vlastním růstem je společnost nucena řešit několik oblastí problémů vznikajících růstem počtu uživatelů, aplikací, počítačem řízených procesů i samotných počítačů.

3.1 Organizačně ekonomický problém

Větší množství využívaných IT prostředků znamená pro organizaci nutnost věnovat víc pozornosti její správě. Tam, kde dřív stačil poučený zaměstnanec, který prováděl základní správu IT prostředků, nyní vzrůstající počet výkonnějších zařízení či aplikací vyžaduje znalosti a zkušenosti. Od managementu roste tlak na nerušený provoz a využívání počítačové techniky. Hledají se tedy organizační opatření, která by zároveň byla i ekonomicky opodstatněná. Možnými přístupy jsou např. zvětšení počtu zaměstnanců IT podpory, jejich vzdělávání, vybavení IT oddělení nástroji usnadňujícími správu, nebo outsourcování správy. Často se volí kombinace těchto přístupů.

HLAVNÍ ZNAKY

- Tlak na ”fungování” IT prostředků – spolehlivost
- Zvýšené množství IT prostředků – méně věcí lze ”držet v hlavě”
- Zatížení IT podpory – víc serverů, PC, tiskáren, routerů
- Růst nákladů na podporu – hledání úspor

3.2 Růst počtu zaměstnanců

Další oblast, které je potřeba věnovat pozornost, je růst počtu zaměstnanců. S každým zaměstnancem se pro firmu pojí mnoho organizačních procesů, které jsou často podporovány IT prostředky. Všech zaměstnanců se týkají procesy ohledně personálního managementu – nástupy, odchody a změny zaměstnaneckého poměru, dále např. nastavení přístupových systémů (dveře, evidence příchodů a odchodů . . .), vydávání obědů . . .

Zaměstnancům, kteří navíc ke své práci používají IT prostředky, je potřeba k těmto prostředkům zajistit přístup, ať už jsou to zařízení, počítače, síťové prostředky nebo aplikace. U všech těchto tříd prostředků je nutné nejen povolit přístup, ale i aplikovat výchozí nastavení, případně omezení práv.

Vyšší počet zaměstnanců také většinou znamená i vyšší dělbu práce a specializaci zaměstnanců. Tím vznikají skupiny uživatelů IT prostředků kteří mají stejné nebo velmi podobné nastavení aplikací, přístupů či práv. Identifikace a využití těchto podobností v podobě organizačních rolí představuje velkou výhodu nejen ve využití při správě identit.

HLAVNÍ ZNAKY

- Počet uživatelů – příchody, odchody, změny
- dělba práce – dělba odpovědnosti
- Tlak managementu na autentičnost IT operací – ”kdo za to může”

3.3 Růst počtu aplikací

Dalším důsledkem růstu společnosti je i růst počtu aplikací které společnost používá. Je to z důvodu specializace jednotlivých oddělení či zaměstnanců, nebo dokonce vynucené vnějším prostředím společnosti.

Jedním ze zdrojů růstu počtu aplikací je právě specializace pracovních pozic. Ta umožní zaměstnancům, aby se víc soustředili na určitou oblast z oboru podnikání společnosti a prováděli ji efektivněji, popřípadě nahradili dodávání výsledků této činnosti jinou společností (služba, subdodávka či outsourcing).

Dalším zdrojem nárůstu počtu aplikací mohou být dodavatelsko-odběratelské vztahy, kde mohou být aplikace vnuceny buď v rámci zefektivnění, usnadnění nebo automatizace komunikace (EDI), nebo jako nutná podmínka ke vzniku takového vztahu (např. dodavatelský řetězec automobilek).

Významný zdroj dalších aplikací je i veřejná správa. Některé úkony, přehledy či oznámení vztahující se ke státní správě, případně ke vztahům vyplývajícím ze zákonných úprav lze, provádět pomocí prostředků IT (někdy výhradně pomocí nich). Často je definovaný přesný formát vyměňovaných informací, případně i aplikace, kterou se úkony mají provádět. Jako příklad mohou soužit datové schránky, celní a daňová správa nebo oblast environmentální.

HLAVNÍ ZNAKY

- vlastní volbou
- vynucená
  - dodavatelé/odběratelé
  - stát

3.4 Bezpečnostní problém

Růst počtu zaměstnanců zvýrazní nutnost vynucení, kontroly a sledování autentičnosti operací, podporovaných IT prostředky. Tam kde – v menších společnostech – bylo jednoduché identifikovat, kdo operaci provedl, ve větším počtu uživatelů je potřeba mechanismy, které vynutí spolehlivou identifikaci. Tuto potřebu má zejména management, který potřebuje pro řízení společnosti identifikovat „kdo za to může“.

Druhá část bezpečnostního pohledu je preventivní. Nastavení nesmí umožnit uživateli získat práva která v součtu mohou vést k – pro společnost – nepříznivým důsledkům. Je například nebezpečné, aby uživatel mohl zároveň přijmout fakturu, schválit ji k proplacení a proplatit.

HLAVNÍ ZNAKY

- autentičnost IT operací
- sady a eskalace uživatelských práv

3.5 Legislativní problém

V některých právních systémech zareagovali na penetraci IT do společnosti a upravují přístup organizací k IT prostředkům a službám. V případě kdy se IdM týká identit subjektů mimo organizaci, mohou údaje podléhat ochraně osobních údajů (v České republice – Zákon č. 101/2000 Sb., o ochraně osobních údajů). Některé podobné dokumenty přímo navrhují konkrétní opatření která společnost má přijmout. Jako příklad uveďme například USA a jeho NSTIC – IDESG Identity ecosystem framework nebo EU – E-Signatures Directive, eID Regulation

Některé doporučené postupy jsou popsány například normou ISO/IEC 27001 (ISO, 2009).

Kapitola 4

Možné přístupy ke správě identit

Účelem této kapitoly je shrnout možné přísupy ke správě identit. Při výčtu postupuji od impementačně nejjednodušších ke složitějším. Stejný postup je většinou při nasazování v praxi, pokud není zvolena cesta studie a hlubší analýzy problému. Taková cesta často ušetří mnoho slepých uliček a nákladných pokusů na provozním prostředí společnosti.

4.1 Vše otevřené – hesla známá všem

Nejjednodušší přístup je správu identit systematicky neřešit. Pokud se používají, jsou použita stejná uživatelská jména a hesla k přístupu ke všem prostředkům. Hesla jsou známá širokému okruhu uživatelů, případně jsou napsána na běžně přístupném místě (monitor, nástěnka . . .)

Z uvedeného vyplývá, že takovéto nastavení „nepravidel“ je nebezpečné a jakékoliv akce prováděné IT prostředky jsou prakticky anonymní.

HLAVNÍ RYSY

- + jednoduché nasazení (nic se nedělá)
- - nebezpečné
- - obtížná kontrola
- - neauditovatelné

4.2 Administrativní opatření

Administrativním opatřením (nařízením, směrnicí) se stanoví pravidla nakládání s IT prostředky a zároveň se stanoví sankce za překročení těchto pravidel. Tento typ správy identit se velmi jednoduše uvádí do praxe, ale velmi obtížně se kontroluje dodržování pravidel. Na porušení pravidel se většinou přijde až v okamžiku kdy se zjišťuje kde nastal v organizaci problém.

HLAVNÍ RYSY

- + jednoduchá nasazení
- - obtížná kontrola

4.3 Technické opatření

Využívají se prostředky k omezení práv a přístupů a to IT prostředků, operačních systémů a aplikací. Nastavení přístupů k IT prostředků se neomezuje jen na uživatelské účty a hesla, ale nastavují se i konkrétní přístupová práva. Obecné IT prostředky a aplikace takovéto nastavení v drtivé většině podporují.

Takováto nastavení se provádí „ručně“, často nesystematicky a podle potřeby. Většinou je možné použít skupiny a nastavovat práva pro skupiny. Někdy má IT personál podpůrné prostředky které udržují informaci o tom jak mají být účty a práva nastavene, ale takováto podpora není automatizovaná.

I přes tuto podporu je možné, že u některých uživatelů může docházet ke kumulaci práv. Jak pracovník v průběhu kariéry střídá pracovní pozice, jsou mu přidělována práva, ale žádná práva mu nejsou odebírána. V průběhu času může získat sadu přístupů která neodpovídá jeho pracovní pozici. Částečně tomu lze předejít používáním skupin.

HLAVNÍ RYSY

- + technicky jednoduché
- + možnost použití skupin
- - nesystematické
- - ruční nastavení
- - čím víc aplikací a uživatelů tím složitější
- - obtížná kontrola
- - nebezpečí kumulace práv

4.4 Adresářová služba

Adresářová služba umožňuje identity a jejich atributy soustředit na jedno místo. To umožní IT oddělení zjednodušit vytváření, mazání a změny identit a řídit přístupová práva na podporovaných IT zařízeních, operačních systémech a aplikacích které to podporují.

Takovéto nastavení práv je vlastně obdoba „technického opatření“ z předchozí kapitoly, s tím, že úložiště identit je spravováno centrálně a na cílových IT prostředcích se nastavují pouze přístupová práva. To přímo vybízí ke zjednodušování administrace přidělováním přístupů v cílových systémech na skupiny uživatelů. Takové nastavení může výrazně omezit nebezpečí kumulace práv

Zásadní nevýhodou tohoto přístupu je nabíledni. Cílový systém či aplikace musí konkrétní adresářovou službu podporovat. U operačních systémů to již většinou není problém, ale u aplikací se situace liší dodavatel od dodavatele.

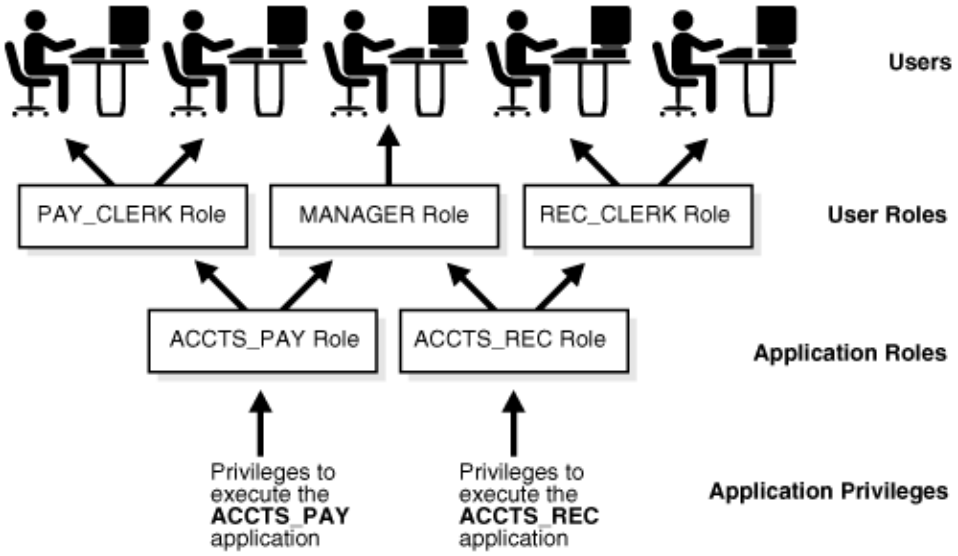
HLAVNÍ RYSY

- + nastavení na jednom místě
- + možnost využívat skupiny
- + možnost využití standardizovaných SSO
- - aplikace to musí podporovat konkrétní adresářovou službu

4.5 Adresářová služba s rolemi

Pokud využijeme adresářovou službu z předchozího článku a budeme striktně aplikovat zjednodušenou obdobu rolí (např. pomocí striktního používání skupin) dostaneme velmi robustní a velmi jednoduše ovladatelný systém správy identit.

Nasazení má dvě úskalí: definování rolí:: definice rolí se neobejde bez spolupráce s personálním oddělením. Pokud tato spolupráce nefunguje nasazení je málokdy úspěšné. kompatibilita aplikací:: pokud aplikace neumožňují využívat adresářovou službu, musí být část identit mimo adresářovou službu.



Obrázek 4.1: Role (Oracle, 2013)

HLAVNÍ RYSY

- + nastavení na jednom místě
- + předem definované role
- + možnost využití standardizovaných SSO
- - aplikace musí podporovat konkrétní adresářovou službu
- - kritická spolupráce s personálním oddělením na definování rolí

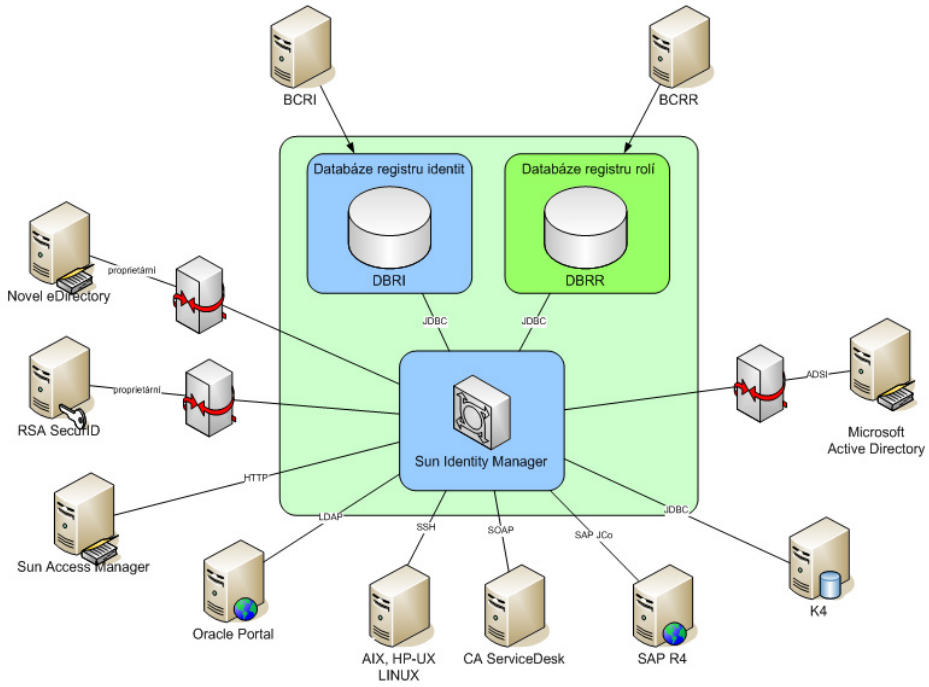
4.6 IdMS

Nasazení identity management systému IdMS umožní v organizaci pracovat s identitami komplexně. Pomocí IdMS lze řídit životní cyklus identit ve všech jeho fázích.

Časté a velice efektivní je napojení IdMS přímo na informační systém personálního oddělení, odkud IdMS čerpá informace o entitách. Na základě těchto informací vytváří v připojených IT prostředcích identity. K vytváření těchto identit se využívají role (např. pracovní zařazení, místo práce . . .).

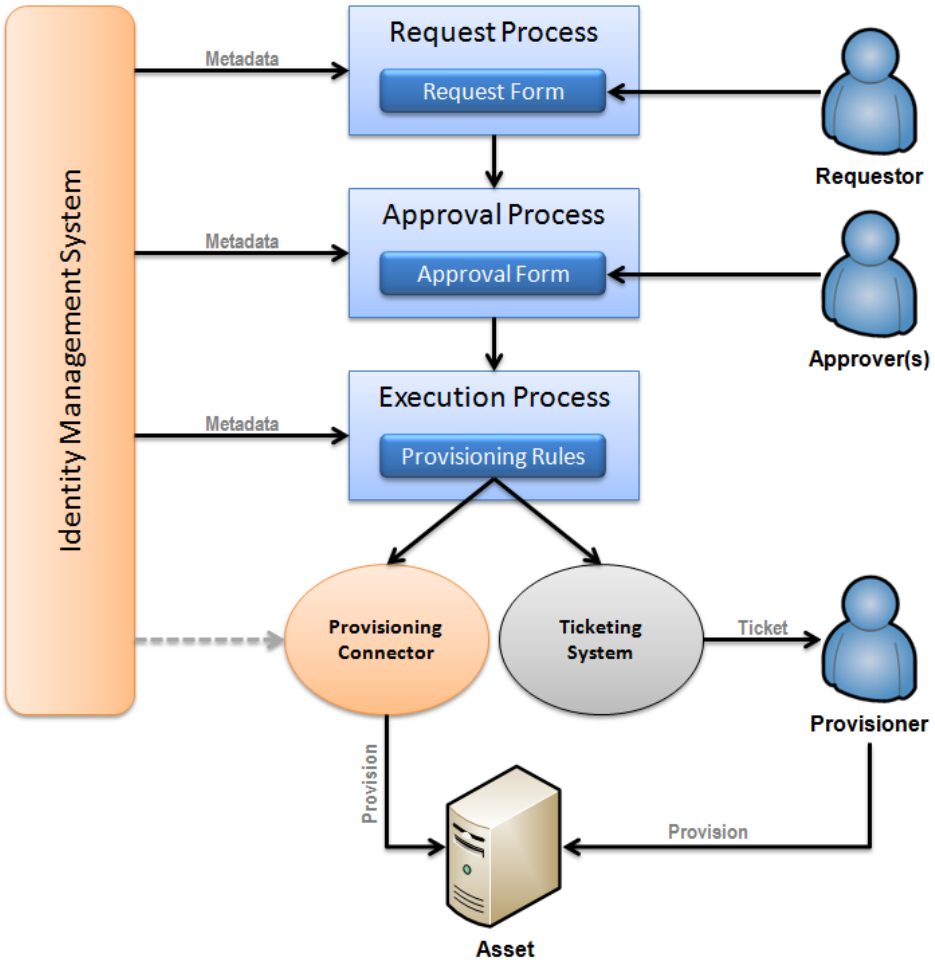
Napojení na cílové IT prostředky je realizováno přes vrstvu konektorů (někdy též agentů). Tato vrstva umožňuje dostatečnou abstrakci, takže umožňuje IdMS využívat ne jen jako zdroj identit pro authorizaci – je často napojen na adresářovou službu

pro prostředky které ji podporují. Může nastavovat práva, přístupy či identity i v systémech, které to neumožňují některým standardizovaným způsobem. Informace o identitách lze také využívat v jiných aplikacích typu telefoní seznam, docházkový systém ...



Obrázek 4.2: IdMS detail (AMI, 2010)

Další důležitá část IdMS je možnost přenesení části administrace identit blíž k uživateli. Pomoci workflow může adminstrátor delegovat některá rozhodnutí (např. nastavení práv, zablokování ...) na nadřízeného žadatele.



Obrázek 4.3: Příklad IdMS workflow (Emden, 2011)

Velmi užitečnou částí IdMS je zpětná kontrola vynucovaných nastavení, atributů identit či práv. Komunikace s cílovými IT prostředky nemusí být jednosměrná a lze definovat reakce na chybné nebo záměrné změny v ovládaných prostředcích.

HLAVNÍ RYSY

- + nastavení na jednom místě
- + definované role
- + možnost napojení všech aplikací – agenty
- + postupné nasazení
- + možnost využití standardizovaných SSO
- - netriviální nastavení
- - kritická spolupráce s personálním oddělením na definování rolí

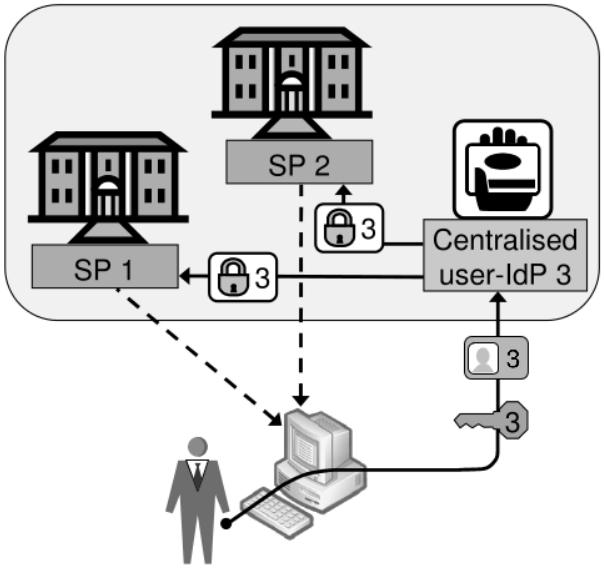
4.7 SSO

Nasazení SSO v plné šíři je vítáno uživateli, protože pro ně přináší výrazný nárůst uživatelského komfortu. Nasazení SSO můžeme uvažovat dvojího druhu:

standardizované SSO jeho implementace je poměrně jednoduchá, za předpokladu, že konkrétní typ SSO aplikace podporují (např. Kerberos . . .)

obecné SSO implementace může být velice náročná, protože, na rozdíl od IdM, neupravuje v aplikacích pouze datové struktury identit, ale i konkrétní authorizační mechanismy

U obecného SSO je důležité zhodnotit přínosy a porovnat je s náklady implementace. Poměrně nenákladně lze SSO implementovat u webových aplikací, případně aplikací, které používají modulární autorizační mechanismus. U ostatních aplikací je nutné autorizační mechanismy upravit, což může být nákladné, až neproveditelné.



Obrázek 4.4: SSO autorizace (Jøsang, Pope, 2005)

HLAVNÍ RYSY

- + vysoký uživatelský komfort
- - riziko velkých zásahů do aplikací

Kapitola 5

Výběr vhodného řešení

V této kapitole se pokusím porovnat možné přístupy ke správě identit a vybrat vhodné řešení pro společnost střední velikosti.

Data o společnosti jsou převzata z reálné společnosti. Z důvodu ochrany potenciálně zneužitelných údajů jí říkejme „X“.

5.1 Údaje o společnosti

Základem pro výběr jsou základní informace o infrastrukruře, vybavení a složení uživatelů společnosti.

Ve společnosti je použito velké množství aplikací, proto vybírám typické zástupce jednotlivých typů aplikací.

ERP Enterprise resource planning – informační systém plánování zdrojů společnosti – základní software řídící základní podnikání společnosti. Běží na OS Unix. Uživatelé k němu přistupují pomocí terminálu přes šifrované spojení SSH

MIS Management information system – informační systém pro plánování a prezentaci konsolidovaných informací. Běží na OS Windows. Skládá se ze serverové a klientské části.

Docházkový systém Zaznamenává a reportuje docházku všech zaměstnanců.

Výdej obědů Umožňuje objednávání, výdej a reportování obědů v jídelně společnosti.

Prvním a základní informací je počet a struktura uživatelů:

Tabulka 5.1: Počty uživatelů a jejich struktura

Struktura uživatelů podle systémů	
Uživatelé ERP	*570*
Uživatelé e-mail	*520*
Uživatelé MIS	*23*
Uživatalé AD	*430*
Uživatelé Linux	*170*
Uživatelé – výdej obědů	*515*
Uživatalé doch. systému	*55*
Identity – doch. systém	*1160*
Celkem uživatelů	*1530*

Zajímavý je také soupis IT prostředků používaných ve společnosti.

Tabulka 5.2: Počty operačních systémů a jejich vlastnosti

systém	počet	možný zdroj identit	SSO	modulární autorizace
windows 7	*93*	*AD*	*Kerberos*	*částečně*
Windows XP	*264*	*AD*	*Kerberos*	*částečně*
Windows Vista	*5*	*AD*	*Kerberos*	*částečně*
Linux	*107*	*LDAP, AD*	*částečně Kerberos*	*ano*
Servery Windows	*6*	*AD*	*Kerberos*	*částečně*
Servery Linux	*8*	*LDAP, AD*	*Kerberos*	*ano*
Servery SUN	*2*	*LDAP, AD*	*Kerberos*	*ano*

Vlastnosti používaných aplikací z pohledu IdM

Tabulka 5.3: Aplikace vyžadující přihlášení nebo nastavení přístupových práv

aplikace	obsahuje identity	využívá identity	SSO	modulární autorizace
Active Directory	*ano*	*ne*	–	–
LDAP Directory	*ano*	*ne*	–	–
Email systém	*ano*	*LDAP*	*ne*	*ano*
MIS	*ne*	*AD*	*AD/Kerberos*	*ne*
ERP	*ano*	*ne*	*ne*	*ano*
docházkový systém	*ano*	*ne*	*ne*	*ne*
výdej obědů	*ano*	*ne*	*ne*	*ano*
telefonní seznam	*ano*	*ne*	–	–

Z uvedeného je zřejmé, že ve společnosti je velmi heterogení prostředí. Na jedné straně jsou stanice a servery s operačními systémy od firmy Microsoft a adresářová služba Active Directory které jsou početně zastoupeny velmi výrazně. Na druhé straně jsou to Unixové servery SUN a stanice a servery s operačním systémem Linux a adresářová služba LDAP.

První skupina je velmi rozšířena v administrativě a podpůrných provozech společnosti. Druhá silně zastoupena ve výrobních a

skladových provozech. Obě skupiny se vzájemně doplňují a z pohledu je takovéto uspořádání výhodné.

U aplikací které nejsou zapojeny do některé z adresářových služeb jsou přístupy a práva nastavována ručně.

Důležitá informace je, že uživatelé mají vlastní uživatelské jméno a heslo. Uživatelé jsou zvyklí na přihlašování do systémů a aplikací.

5.2 Porovnání přístupů

Porovnáním možných přístupů ke správě identit, současného a potenciálně cílového stavu, se budu snažit eliminovat ty přístupy, které nejsou vhodné a naopak identifikovat ty, které jsou výhodné.

5.2.1 Vše otevřené – hesla známá všem

Zavedení tohoto způsobu správy identit by bylo velmi jednoduché, ale v současném stavu správy identit ve společnosti by to byl krok zpět. Ve společnosti je již v provozu Active Directory a LDAP adresářová služba. Navíc v organizaci vládne vysoká specializace a potřeba, zvlášť při vysokém počtu transakcí, autenticity IT operací je silná.

VÝHODY

- velice jednoduché nasazení

NEVÝHODY

- ztráta autenticity operací
- nemožná kontrola odpovědnosti
- extrémně nízké zabezpečení

5.2.2 Administrativní opatření

Důvody pro zamítnutí tohoto způsobu jsou podobné jako v předchozím případě. Současný stav je směs používání adresářových služeb a diskrétních nastavení. Některá opatření mají ráz administrativního opatření (např. že se uživatel nesmí přihlásit na cizí uživatelské jméno), ale globálně je správa identit na vyšší úrovni.

VÝHODY

- jednoduché nasazení

NEVÝHODY

- obtížná kontrola dodržování
- ztráta autenticity operací
- nemožná kontrola odpovědnosti
- nízké zabezpečení

5.2.3 Technické opatření

Současný stav je v porovnání s řešením správy identit technickými opatřeními v některých částech shodný. Některé aplikace mají přístupy a práva nastavována ručně. Dále má IT oddělení nastavený proces přidělování práv tímto způsobem i do adresářových služeb. I přes to je takovéto nastavení obtížně kontrolovatelné.

VÝHODY

- technicky jednoduché
- možnost použití skupin

NEVÝHODY

- nesystematické
- ruční nastavení
- náročnost roste s počtem aplikací
- obtížná kontrola
- nebezpečí kumulace práv

5.2.4 Adresářová služba, Adresářová služba s rolemi

Správa identit založená čistě na adresářové službě ve společnosti nelze použít. V organizaci jsou používané aplikace které nepodporují adresářové služby.

Problém je i používání dvou adresářových služeb. Obě jsou LDAP kompatibilní, ale ze zkušeností není radno mixovat Active Directory a LDAP pro Unix. Proto i nadále zůstanou obě.

VÝHODY

- nastavení na jednom místě
- možnost použití skupin
- možnost využití standardizovaných SSO

NEVÝHODY

- aplikace musí podporovat konkrétní adresářovou službu
- ruční synchronizace AD a LDAP

5.2.5 Adresářová služba s rolemi + Technické opatření

Kombinovaný přístup – adresářová služba + ruční nastavení práv (technické opatření) pokrývá všechny možné varianty. Pak by se dalo dosáhnout téměř konzistentní správu identit.

Ruční synchronizace AD a LDAP je jedna ze zjevných nevýhod tohoto řešení, stejně jako nebezpečí kumulace práv u ručních nastavení aplikací.

VÝHODY

- nastavení na jednom místě
- možnost použití skupin
- možnost využití standardizovaných SSO
- pokrytí všech aplikací

NEVÝHODA

- ruční nastavení
- náročnost roste s počtem aplikací
- obtížná kontrola
- nebezpečí kumulace práv
- ruční synchronizace AD a LDAP

Nevýhody lze zmenšit postupným nahrazováním aplikací které nepodporují žádnou adresářovou službu.

5.2.6 IdMS

Nasazení IdMS umožní vyřešit nejen synchronizaci adresářových služeb, ale i diskrétní nastavení aplikací které nepodporují žádnou adresářovou službu.

IdMS není bez nevýhod, kromě nákladů (finančních, personálních ...) si částečně vynutí zněny v procesech společnosti a to především při spolupráci s personálním oddělením.

VÝHODY

- nastavení na jednom místě
- možnost použití skupin a rolí
- možnost využití standardizovaných SSO
- pokrytí všech aplikací
- možnost postupného nasazení
- snadná kontrola a reportování
- workflow a delegování administrace

NEVÝHODY

- vysoké náklady (finanční, personální ...)
- nutnost upravit procesy personálního oddělení

5.2.7 SSO

Nasazení SSO by bylo třešničkou na dortu, ale jeho nasazení je komplikováno heterogení m prostředím IT prostředků. SSO Kerberos je podporováno všemi operačními systémy, ale podpora u aplikací není úplná a tak je na zvážení zda toto SSO nasazovat. Jiný SSO by si vyžádal vysoké náklady a proto bych jeho případné nasazení odložil až po úspěšné implementaci IdMS.

VÝHODY

- uživatelský komfort

NEVÝHODY

- neúplná podpora aplikací

5.3 Shrnutí

Přístupy ke správě identit se liší v jednotlivých oblastech. Pro jasnější přehled jsou tyto vlastnosti shrnuty v následujících tabulkách.

Tabulka 5.4: Shrnutí vlastností jednotlivých metod (část 1.)

Oblast	Vše otevřené – hesla známá všem	Administrativní opatření	Technické opatření	Adresářová služba	Adresářová služba s rolemi
Technická složitost	*velmi nízká*	*velmi nízká*	*nízká*	*střední*	*střední*
Náklady pořízení	*velmi nízké*	*velmi nízké*	*velmi nízké*	*nízké (bývá součástí OS serveru)*	*nízké (bývá součástí OS serveru)*
Bezpečnost	*velmi nízká*	*nízká*	*střední*	*střední*	*střední*
Podpora více OS	*vysoká*	*vysoká*	*vysoká*	*střední*	*střední*
Kontrola dodržování nastavení	*velmi nízká*	*velmi nízká*	*nízká*	*střední*	*střední*
Provozní zátěž oddělení IT	*velmi nízká*	*nízká*	*vysoká*	*střední*	*střední*
Možnost automatizace	*velmi nízká*	*velmi nízká*	*nízká*	*střední*	*střední*
Nebezpečí kumulace práv	*práva nejsou nastavována*	*práva nejsou nastavována*	*vysoká*	*střední*	*nižší*
Využití skupin	*práva nejsou nastavována*	*práva nejsou nastavována*	*ano*	*ano*	*ano*
Využití rolí	*práva nejsou nastavována*	*práva nejsou nastavována*	*ne*	*ne*	*ano (udržováno ručně)*
Centralizace nastavení	*není*	*není*	*není*	*ano*	*ano*
Omezení jen na podporované aplikace	*není*	*není*	*není*	*ano*	*ano*
Potřeba externí spolupráce	*není*	*není*	*není*	*ne*	*ano (definování rolí)*
SSO	*není*	*není*	*není*	*jen podporované prostředky*	*jen podporované prostředky*

Tabulka 5.5: Shrnutí vlastností jednotlivých metod (část 2.)

Oblast	**Adresářová služba s rolemi + Technické opatření**	**IDM**	**Standardizované SSO**	**Obecné SSO**
Technická složitost	*střední*	*vysoká*	*střední*	*vysoká*
Náklady pořízení	*nízké (bývá součástí OS serveru)*	*vysoké*	*nízké (bývá součástí OS serveru)*	*střední*
Bezpečnost	*střední*	*vysoká*	*vyšší*	*vyšší*
Podpora více OS	*střední*	*vysoká*	*střední*	*vysoká*
Kontrola dodržování nastavení	*vyšší*	*vysoká*	-	-
Provozní zátěž oddělení IT	*vyšší*	*nízká*	*nízká*	*nízká*
Možnost automatizace	*střední*	*vysoká*	-	-
Nebezpečí kumulace práv	*nižší*	*nízké*	-	-
Využití skupin	*ano*	*ano*	-	-
Využití rolí	*ano (udržováno ručně)*	*ano*	-	-
Centralizace nastavení	*ano*	*ano*	*ano*	*ano*
Omezení jen na podporované aplikace	*ne*	*ne*	*ano*	*ne*
Potřeba externí spolupráce	*ano (definování rolí)*	*ano (definování rolí a workflow)*	*ne*	*ne*
SSO	*jen podporované prostředky*	*je možné*	*jen podporované prostředky*	*ano*

5.4 Výběr řešení

Na základě známého stavu IT prostředků ve společnosti a zhodnocení vlastností jednotlivých způsobů správy identit je možno vybrat vhodný způsob.

V následujících tabulkách jsou shrnuty vlastnosti za pomoci následujících symbolů:

++ výrazné zlepšení

+ zlepšení

0 žádné/nevýrazné zlepšení

- zhoršení

-- výrazné zhoršení

/ nelze použít, nelze porovnat

Tabulka 5.6: Přínosy jednotlivých metod v porovnání se současným stavem (část 1.)

Oblast	Stav správy identit ve společnosti	Vše otevřené – hesla známá všem	Administrativní opatření	Technické opatření	Adresářová služba
Technická složitost	*střední*	++	++	+	*0*
Náklady pořízení	*nízké*	+	+	+	*0*
Bezpečnost	**střední**	**—**	**-**	**0**	**0**
Podpora více OS	*vysoká*	*0*	*0*	*0*	-
Kontrola dodržování nastavení	**střední**	**—**	**—**	**-**	**0**
Provozní zátěž oddělení IT	**střední**	**++**	**+**	**—**	**0**
Možnost automatizace	**střední**	**—**	**—**	**-**	**0**
Nebezpečí kumulace práv	*střední*	++	++	-	*0*
Využití skupin	*ano*	-	-	*0*	*0*
Využití rolí	**ne**	**-**	**-**	**0**	**0**
Centralizace nastavení	**ano**	**-**	**-**	**-**	**0**
Omezení jen na podporované aplikace	*ano*	*/*	*/*	*/*	*0*
Potřeba externí spolupráce	*ne*	*/*	*/*	*/*	*0*
SSO	*jen podporované prostředky*	-	-	-	*0*

Tabulka 5.7: Přínosy jednotlivých metod v porovnání se současným stavem (část 2.)

Oblast	Stav správy identit ve společnosti	Adresářová služba s rolemi	Adresářová služba s rolemi + Technické opatření	IdMS	Standardizované SSO	Obecné SSO
Technická složitost	*střední*	*0*	*0*	--	*0*	--
Náklady pořízení	*nízké*	*0*	*0*	--	*0*	-
Bezpečnost	**střední**	**0**	**0**	**++**	**+**	**+**
Podpora více OS	*vysoká*	-	-	*0*	-	*0*
Kontrola dodržování nastavení	**střední**	**0**	**+**	**++**	**/**	**/**
Provozní zátěž oddělení IT	**střední**	**0**	**-**	**++**	**++**	**++**
Možnost automatizace	**střední**	**0**	**0**	**++**	**/**	**/**
Nebezpečí kumulace práv	*střední*	+	+	++	/	/
Využití skupin	*ano*	*0*	*0*	*0*	/	/
Využití rolí	**ne**	**+**	**+**	**++**	**/**	**/**
Centralizace nastavení	**ano**	**0**	**0**	**0**	**0**	**0**
Omezení jen na podporované aplikace	*ano*	*0*	+	++	*0*	+
Potřeba externí spolupráce	*ne*	-	-	-	*0*	*0*
SSO	*jen podporované prostředky*	*0*	*0*	+	*0*	++

V tabulkách jsou vyznačeny důležité vlastnosti, které jsou zajímavé pro management. Management je ten který v organizacích rozhoduje o změnách v procesech.

Z pohledu srovnání přínosů se **IdMS** pro organizaci jeví jako zajímavá volba.

Navíc, v literatuře se mezi bázové rysy správy identity zahrnuje (Hanáček, Staudek, 2005):

- Centralizovaná administrace pomocí www aplikace
- Možnost delegování administrativních úkonů na bázi definovaných rolí a pravidel
- Možnost provádět manipulace s hesly uživateli samoobslužně, bez intervence centrální administrativy
- Dostupnost inteligentního směrování schvalovacích postupů při vyřizování žádostí o přístup ke zdrojům
- Automatizované aktivování prostředí jednotlivých uživatelů
- Dostupnost auditních mechanismů a mechanismů pro automatické generování přehledových zpráv (kdo má k čemu přístup)

K těmto vlastnostem se výrazně přibližuje **IdMS**, který při plném rozvinutí může splnit všechny uvedené body.

Proto je to právě **IdMS** které jsem vybral jako vhodnou metodu pro implementaci.

Kapitola 6

Zásady implementace

Výběr konkrétního IdMS je závislý na kombinaci ovládaných IT prostředků, preferenci běhového prostředí, komfortu obsluhy a samozřejmě ceně.

NEJPOUŽÍVANĚJŠÍ IDMS

- Microsoft Identity Integration Server
- Sun Identity Manager a z něj vycházející OpenIDM
- Oracle Identity Manager
- IBM Tivoli Identity Manager

Výběr konkrétního IdMS je mimo záběr této práce.

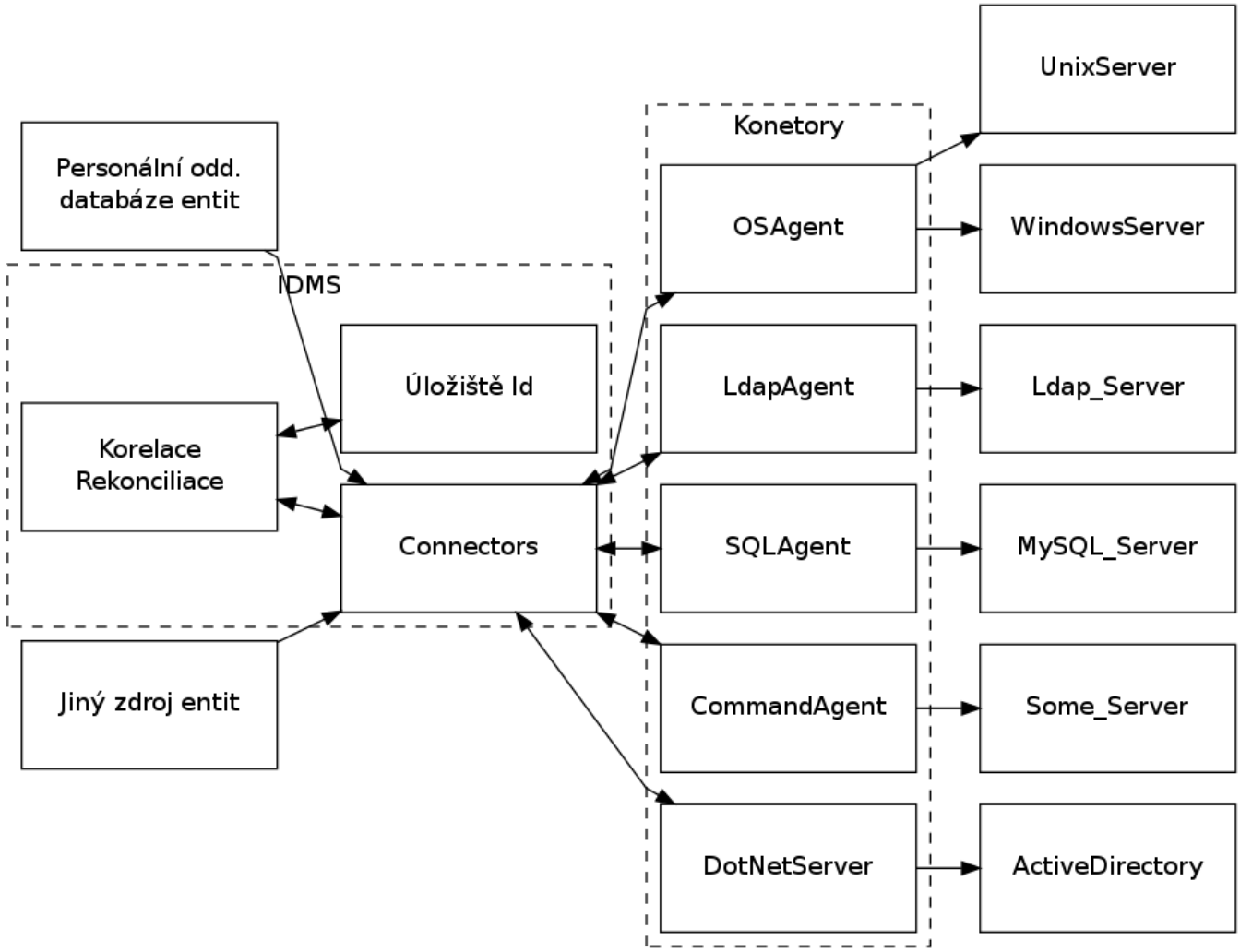
Výběrem IdMS však implementace teprve začíná. Naštěstí, výrazným rysem tohoto řešení je, že ho lze nasazovat postupně. Při implementaci lze zdroje připojovat v režimu pouze pro čtení a využít reportovací schopnosti IdMS ke hlášení neshod. Po jejich odstranění je možno systém přepnout do režimu plného přístupu.

POSTUP PŘI IMPLEMENTACI

- Při implementaci je důležitá spolupráce s personálním oddělením, které ve spolupráci s ostatními odděleními definuje uživatelské role.
- Od personálního oddělení také většinou pochází databáze identit. Často se však používají i další zdroje identit.
- Po načtení entit do IdMS je možné nastavit ke čtení první zdroj, případně nastavit korelační a rekonciliační pravidla.
  - IdMS se pokusí o korelaci a rekonciliaci identit v IdMS a identit které jsou ve zdroji.
  - Tam kde narazí na neshody a neřešitelné konflikty využije reportovací možnosti IdMS k jejich nahlášení.
  - Opravováním dat v úložištích nebo upravováním pravidel, se neshody postupně odstraňují.
  - Po odstranění všech neshod je možné zdroj připojit do režimu pro zápis a plného provozu.
- Tímto způsobem lze postupně přidávat i další zdroje.
- Cílový stav je připojit všechny zdroje (adresářové služby, systémy, aplikace . . .)

SOUBĚŽNÉ KROKY

- nastavení reportingu neshod – včas upozorní na problémy
- definování rolí
- aplikování rolí
- workflow žádosti o přístup ke zdrojům
- exporty (např. telefonní seznam)



Obrázek 6.1: Schéma obecného IdMS

Nastavení jednotlivých IdMS se liší co do způsobu nebo komfortu, tyto zásady jsou však platné pro všechny z nich.

Kapitola 7

Závěr

V práci jsou shrnuty možné přístupy ke správě identit, jejich silné i slabé stránky. Pro společnost s heterogením IT prostředím a dannými omezeními, se jako nejvýhodnější jeví nasazení IsMS. Porovnáním různých přístupů ke správě IdM lze u jiné společnost dojít k jinému výsledku. Vyhotovený přehled a závěry této práce mohu být využity při rozhodování o výběru způsobu správy identit v organizacích střední velikosti.

Nasadit IdM ve společnosti v plné šíři je víc strategicko organizační rozhodnutí, než technický projekt firemního IT oddělení. Úspěšná implementace vyžaduje úzkou spolupráci přes všechna oddělení společnosti.

IT technicky zajišťuje a organizačně koordinuje spolupráci. Oddělení lidských zdrojů dodává informace o stávajících zaměstnancích, o příchodech, odchodech a změnách. Zároveň ve spolupráci ostatními odděleními definuje role a jejich obsah pro použití v IdM. Právní oddělení posuzuje shodu s legislativním prostředím, pokud je požadována. Ostatní oddělení spolupracují při definování rolí a to jak vlastních zaměstnanců společnosti, tak i rolí externích spolupracovníků a dodavatelů.

Z uvedeného vyplývá, že pro úspěšné nasazení je potřeba, aby sponzor projektu byl co nejvýš ve firemní hierarchii. Takto uchopený projekt má šanci uspět ve všech důležitých oblastech – zjednodušení správy a zvýšení bezpečnosti.

Zjednodušení/zlevnění správy identit odlehčí IT od rutinních úkonů a uvolní kapacity pro rozvoj lepšího užití výpočetní techniky ve společnosti. Zároveň se zvýší bezpečnost protože IT má automatizovaný nástroj na kontrolu, nastavení a vynucování bezpečnostních pravidel organizace spojených s identitami a přístupy k informacím.

Z těchto důvodů nutně docházím k závěru, že investice prostředků a práce do impementace IdM se podniku střední velikosti vyplatí a mohu ji jen doporučit.

Kapitola 8

Zdroje

Seznam doporučené literatury

- BERTINO, Elisa a Kenji TAKAHASHI. Identity management: concepts, technologies, and systems. Boston: Artech House, 2011, 196 pages. Artech House information security and privacy series. ISBN 16-080-7039-5.
- BISHOP, Matt. Computer security: art and science. Boston: Addison-Wesley, 2003, xli, 1084 p. ISBN 02-014-4099-7.
- HANÁČEK Petr, STAUDEK Jan. Správa identity. In: Sborník konference DATAKON 2005. Brno: MUNI [online]. 2005 [cit. 2013-01-29]. ISBN 80-210-3813-6. [dostupné online http://www.buslab.org/download/kib/d05_idm_tutorial_text.pdf]
- PFITZMANN, Andreas a Marit HANSEN. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. [online]. 2010 [cit. 2013-04-13]. Dostupné z: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

Publikace

- HARROP Mike. Identity management. Security Workshop, 2009-01. 2009. Dostupné z: http://docbox.etsi.org/workshop/-2009/200901_SECURITYWORKSHOP/TheCottinghamGroup_Harrop_IdentityManagement.pdf
- JØSANG Audun, POPE Simon. User centric identity management. In: AusCERT Asia Pacific Information Technology Security Conference. 2005 [cit. 2013-04-13]. p. 77. Dostupné z: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=re
- NABETH, Tiery. Identity of Identity. Datenschutz und Datensicherheit 9/2006. pp. 538-542, Wiesbaden. 2006 [cit. 2013-04-13]. Dostupné z: http://fw-wwwcalt.insead.edu/project/Fidis/documents/2006-Fidis-Journal-WP2.pdf

Standardy

- CCITT. The Directory: Overview of Concepts, Models and Service. CCITT Recommendation X.500, 1988 [cit. 2013-01-29]. Dostupné z: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.500-200811-I!!PDF-E&type=items
- ISO. Information Processing Systems – Open Systems Interconnection – The Directory: Overview of Concepts, Models and Service. ISO/IEC JTC 1/SC21; International Standard 9594-1. 2011
- ISO. Information Technology — Security Techniques — A Framework for Identity Management. ISO/IEC WD 24760 (Working draft). 2009

- ITU-T. Identity Management Framework. ITU-T Recommendation, Y.2720. 2009 [cit. 2013-04-13]. Dostupné z: http://www.itu.int/-rec/dologin_pub.asp?lang=e&id=T-REC-Y.2720-200901-I!!PDF-E&type=items
- SERMERSHEIM, Jim. RFC 4511-Lightweight Directory Access Protocol (LDAP): The Protocol. Internet Engineering Task Force, TechRep [online]. 2006 [cit. 2013-01-29]. Dostupné z: http://www.ietf.org/rfc/rfc4511.txt

WWW STRÁNKY

- AMI Praha a.s. Identity management. [online]. 2010 [cit. 2013-01-29]. Dostupné z: http://www.ami.cz/reference/identity-management-cez-ict-services
- Aphroland. Lightweight Directory Access Protocol. [online] .2013 [cit. 2013-01-29]. Dostupné z: http://www.aphroland.de/-LDAP.htm
- EMDEN Toby. Decomposing Identity Management Approval Workflows. [online]. 2011 [cit. 2013-01-29]. Dostupné z: http://evolvingi 2011/10/decomposing-identity-management.html
- JUSTUS Ioana Bazavan. Identity Management Series – Role and Rule Basing Part 1: Introduction. Michael Santarcangelo, THE SECURITY CATALYST [online]. 2010 [cit. 2013-01-29]. Dostupné z: http://www.securitycatalyst.com/role-and-rule-basing-part-1-introduction/
- Oracle. Database Concepts 11g Release 2 – Topics for Database Administrators and Developers. [online] . 2013 [cit. 2013-01-29]. Dostupné z: http://docs.oracle.com/cd/E11882_01/server.112/e16508/cmntopc.htm
- SNOCK Daniel. Kerberos negotiations. [online]. 2011 [cit. 2013-01-29]. Dostupné z: http://upload.wikimedia.org/wikipedia/-commons/4/4e/Kerberos.svg

Kapitola 9

Rejstřík