Správa identit a přístupů v informačních systémech

Aleš Tesáček

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Aleš Tesáček**
Osobní číslo:	**A14212**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Správa identit a přístupů v informačních systémech**
Téma anglicky:	**Identity and Access Management in Information Systems**

Zásady pro vypracování:

1. **Proveďte literární rešerši tématu správy identit a přístupů v informačních systémech.**
2. **Analyzujte možnosti a požadavky na správu identit a přístupů.**
3. **Navrhněte vhodný způsob implementace správy identit.**
4. **Navrhněte vhodnou formu řízení přístupů v informačním systému.**
5. **Vyhodnoťte své návrhy v konfrontaci s praxí a případovými studiemi.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **BLANCHARD, Benjamin S. a John BLYLER. System engineering management. Fifth edition. Hoboken, New Jersey: Wiley, 2016. ISBN 9781119047827.**
2. **DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.**
3. **GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015, 240 s. Management v informační společnosti. ISBN 978-80-247-5457-4.**
4. **GALBA, Alexander a Antonín PAVLÍČEK. Moderní informatika. Praha: Professional Publishing, 2012, 184 s. ISBN 978-80-7431-095-9.**
5. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821**
6. **SOMMERVILLE, Ian. Softwarové inženýrství. Brno: Computer Press, 2013, 680 s. ISBN 9788025138267.**

Vedoucí bakalářské práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **15. prosince 2017**

Termín odevzdání bakalářské práce: **25. května 2018**

Ve Zlíně dne 15. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považuji se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 21.5.2018

.....
podpis diplomanta

ABSTRAKT

Bakalářská práce je zaměřena na analýzu přístupu ke správě identit v informačních systémech a její aplikaci v malých a velkých firmách. Práce je rozdělena do 5 částí. V teoretické části provádím rešerši správy identit a přístupů v informačních systémech. V praktické navrhuji optimální způsob implementace správy identit a vhodnou formu řízení přístupů v informačním systému.

Klíčová slova: IAM, LDAP servery, Biometrické zabezpečení, Active Directory

ABSTRACT

Bachelor thesis is focused on analysis of approach to the identity management in information systems and its application in small and large companies. Thesis is divided into 5 parts. The theoretical part describe Identity and Access management in Information Systems. In practice, I propose the optimal way to implement Identity management and appropriate form of Access Management information system.

Keywords: IAM, LDAP servers, Biometric autorization, Active Directory

Rád bych poděkoval vedoucímu bakalářské práce, Prof. Mgr. Romanu Jaškovi, Ph.D. za odborné rady, připomínky a pomoc v průběhu tvorby této bakalářské práce.

Motto:

„ Věda má svůj smysl, pokud se chápe jako cesta k pravdě a pravda jako dobro člověka. „

Jan Pavel II.

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Všestranný rozvoj vědy a techniky se promítá do mnoha oblastí našeho života.

Vědecko-technický vývoj nás provází na každém kroku, působí značnou měrou na komerci a naopak komerce má vliv na technický vývoj a tím i na správu identit a přístupů k nim.

V digitální ekonomice vytváří digitální komunikační a informační infrastruktura globální podnikatelskou a společenskou platformu, ve které lidé a organizace vzájemně komunikují a spolupracují.

Digitální ekonomika je charakteristická širokou nabídkou a poptávkou po digitálních produktech zahrnující databáze informací, elektronické knihy a časopisy, software atd.

V digitální ekonomice fungují i fyzické produkty v podobě mikroprocesorů s možností připojení do komunikační sítě, tj. v rámci digitální infrastruktury (doprava, energetika, zdravotnictví atd.). Dochází zde ke konvergenci výpočetní a komunikační techniky, která podporuje výměnu informací a poptávku po digitálních produktech a přeměnu téměř všech běžných činností do digitální podoby. Vzniká prostor pro elektronické podnikání (e-business), obchodování (e-commerce) a pro digitalizaci veřejné správy (e-government). Problémem současného IS/ICT[1] jsou vysoké náklady, které se někdy investují zbytečně do nepotřebných funkcí a předražených řešení. Firmy se občas snaží snížit cenu tím, že neuvedou všechny náklady, které s daným řešením souvisí. IdM/IAM produkty těchto firem překročí stanovený rozpočet. Jednou z příčin je nedostatek kvalifikovaných IT odborníků.

V současné době dochází k velkým změnám v IT/ICT v důsledku zrychlování vývoje technologií, zvyšování výpočetní a paměťové kapacity celého spektra zařízení od mobilních technologií po stacionární PC/Servery, a tím dochází ke stále kratší morální životnosti hardwarového i softwarového vybavení.

Zůstává pouze otázka, zda se vyplatí podnikům investovat do nového rychlejšího hardwarového vybavení, když málokterý uživatel využije plnou kapacitu svého dosavadního zařízení. Jedním z výrazných trendů v IT/ICT je snaha o integraci různorodých systému.

[1] Informační a komunikační technologie – používá se i česká zkratka IKT.

Tento trend je potřebou spojení systému mezi sebou. Centralizací se zabývá systémová integrace
a problematiku centralizace dat řeší datové sklady (Data Warehouse). Trend integrace se řeší v rovině celopodnikových systémů **ERP** (Enterprice Resource Planning).

Správa identity je souhrn služeb, které poskytují bezpečné automatizované přístupy k informačním zdrojům. Technologicky je tato integrace řešena **SOA** (Service Oriented Architecture).

Celopodnikové informační systémy **ERP** sdružují celou řadu aplikačních softwarových programů, které umožňují řízení a koordinaci podnikových zdrojů a aktivit (plánování, účetnictví apod.).

Komponenty **ERP**:

- ERP software
- Podnikové procesy
- Uživatelé
- HW i OS

IdM je soubor nástrojů, který se zabývá správou entit. Identita entity (uživatel, zaměstnanec atd.) je vyjádření její totožnosti. Identifikace je určení, které opravňuje uživatele k přístupu a zároveň řídí jeho práva (profil). K tomuto tématu se vztahuje i digitální identita, známá pod pojmem ID (adresa, výsady atd.).

Cílem bakalářské práce je analýza přístupu a správy identit pro malé podniky.

Postup práce a použité metody

Práce je rozčleněna do 5 kapitol. Při vypracování jsem vycházel z vlastní praxe, anglických i českých vědeckých článků a informací z webových stránek.

V teoretické části se zaměřuji na rešerši správy identit a přístupů v informačních systémech, analyzuji možnosti a požadavky na jejich správu. V praktické části navrhuji optimální způsob implementace a vhodnou formu řízení přístupů v informačním systému. V závěru hodnotím své návrhy v konfrontaci s praxí a případovými studiemi.

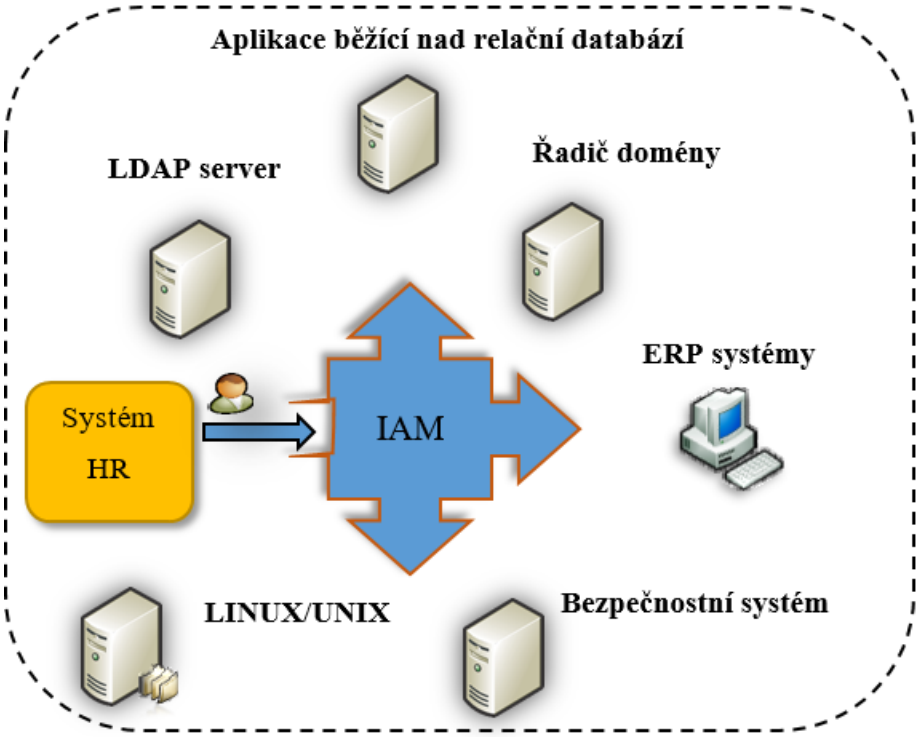
Práce má charakter výzkumu „ od stolu“ (desk research).

I. TEORETICKÁ ČÁST

1 SPRÁVA UŽIVATELSKÝCH IDENTIT

1.1 IAM

Správa pro řízení identit je postavena na práci s identitami, které vyjadřují reálné entity a jsou přímými nebo nepřímými účastníky v celém systému.



Obr. 1. Architektura IAM [2]

Správa identit a přístupů (**I**dentity and **A**ccess **M**anagement) je relativně široká oblast, složená z mnoha spolupracujících technologií.

Poznámky ke schématu: HR systém – Systém lidských zdrojů (centralizuje a zabezpečuje data zaměstnanců), ERP – viz úvod, LINUX/UNIX (OS).

[2] Vlastní tvorba na základě článku SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (5. díl): Architektura IAM řešení. [1]

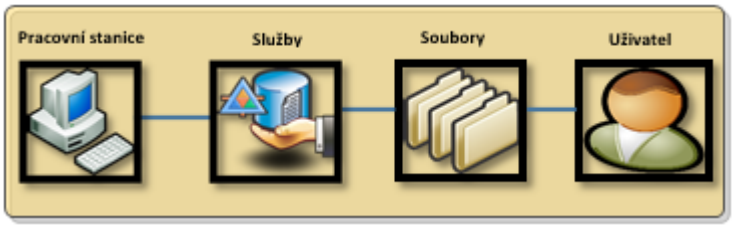
Prvky řešení se kombinují přesně podle potřeb určitého prostředí, proto jsou variabilní.

Základ IAM tvoří:

- ***Adresářová služba*** (Directory Service) udržuje centrální databázi uživatelů
- ***Systém řízení přístupu*** (Access Management) vykonává centrální autentifikaci (SSO), základní autorizaci (Audit) přístupů.
- ***Provisioning systém*** zabezpečuje správu databáze uživatelů, synchronizaci (lidské zdroje) a přiřazuje bezpečnostní politiku.

Tyto technologie se navzájem doplňují.

Adresářová služba u menších podniků (Active Directory)



Obr. 2. Active Directory – základní koncept[3]

U větších podniků se používá systém dedikovaných LDAP serverů.

Základní princip u obou technologií je stejný.

Adresářová služba je specializovaná databáze uživatelů a obsahuje údaje o identitách. Jsou zde speciální atributy pro heslo, fotografii apod.

Základem každého IAM řešení je nalezení vhodné adresářové služby. Důležitým bodem pro efektivní koncept IAM je použití adresářové služby pouze jako databáze, která

[3] Vlastní tvorba na základě článku „Active Directory: Concepts Part 1“. [2]

přenechává logiku ostatním technologiím. Nedostatky adresářových služeb řeší systémy na správu přístupu (AM – Access Management).

AM se skládá z technologií jednotného přihlašování (Single Sign On - SSO) a současně i z různých autorizačních a autentizačních technologií.

Tyto technologie se zabývají problémy, které mohou nastat v tradičních aplikacích, kdy autentizaci, autorizaci a další bezpečnostní mechanismy se implementují samostatně. Provozovatel musí platit za funkce několikrát, nejen za jejich vývoj, ale i za konfiguraci a provoz. Jednotlivé aplikace na sebe navzájem nenavazují a uživatel se musí přihlásit do každé aplikace zvlášť.

SSO nebo AM server zabezpečuje uživateli možnost zadat heslo jen při prvním přístupu k některé z itengrovaných aplikací. V tomto případě je uživatel přesměrován na SSO server, kde se pomocí svých přihlašovacích údajů autentizuje. Dokud se uživatel neodhlásí z některé aplikace nebo nepřekročí definovaný čas nečinnosti, může pracovat s aplikací bez nutnosti opětovného přihlášení. Systém na správu identit (IdM) je využíván k unifikaci databází uživatelů jednotlivých aplikací a vytvoření centrální databáze adresářovým systémem. Produktů, které jsou určeny k řízení přístupů, je velké množství a jsou to finančně náročné investice.

AM vykonává autentizaci uživatele a dokáže i částečně autorizovat jeho přístup. Všechny přístupy jsou logovány a slouží pro účely auditu i pro zjednodušení přihlašování.

Moderní AM řešení implementují identity mezi organizacemi a integraci i na sociální sítě (GoogleID, Facebook atd.). Pokud má systém AM dobře pracovat, musí mít k dispozici sjednocenou databázi uživatelů. Pro mnoho organizací je náročné i základní zabezpečení přihlašovacích údajů uživatelů, a proto dochází ke krádeži identit. [3]

Sjednocování databází má za úkol řešit poslední komponenta – ***Provisioning systém***, který sychronizuje údaje v adresářové službě v personálních systémem a v různých aplikacích.

Tento systém, který provádí konzistenci databází je nejdůležitějším komponentem IAM řešení. Aplikuje bezpečnostní politiku, transformuje údaje, řídí pracovní procesy, poskytuje samoobslužné služby apod.

Je nemožné sestavit plnohodnotné IAM řešení bez kteréhokoliv komponentu.

S rozvojem technologií v současnosti dochází k velkým změnám v IAM, hlavně díky cloudovým technologiím, mobilním zařízením i sociálním změnám.

Předpokládá se, že do roku 2020 bude přístup uživatelů ovlivňován novou mobilní architekturou, která nebude založená na klasické PC architektuře a která zároveň bude stírat rozdíl mezi soukromou a pracovní identitou. [4]

1.2 Technologie pro správu identit

Technologie (IT) – využití teoretických vědomostí při praktickém řešení. Podporuje shromažďování, přenos, záznam, organizaci, vyhledávání a zpřístupňování informací zejména prostředky výpočetní techniky a telekomunikací. [5]

Softwarové systémy zpracovávají data a informace, které mají velkou hodnotu pro podnik.

Tvoří nehmotnou a nedílnou součást PC, jsou to programy respektive aplikace počítačového systému. Softwarová architektura je v současné době vrstvená založená na principu sdružování podobných funkcí do určitých subsystémů, které jsou od sebe oddělené a relativně nezávislé. Podle této architektury došlo k oddělení subsystému pro práci s daty od subsystému pro vlastní zpracování dat a subsystému uživatelského rozhraní. Subsystém pro práci s daty je označován jako databázový systém a umožňuje definování struktury dat.

Hlavním úkolem pro subsystém zpracování dat je aplikovat pravidla a transformovat data podle daných požadavků a potřeb. Tento subsystém je označován jako aplikační nebo firemní logika. Subsystém uživatelského rozhraní je určen k zadávání různých příkazů a prezentování výsledků. Je nazýván prezentační vrstvou, která může být zprostředkována pomocí příkazového řádku, GUI apod.

Příklad jednoduché vrstvené architektury je např. Klient – Server.

Technologie pro adresářové služby:

a) **ASN.1 (Abstract Syntax Notation One)**
   - používá se pro popis datových struktur, pro reprezentaci, kódování, přenos, ukládání a dekódování dat v počítačových a telekomunikačních sítích. Pro přenos dat po síti je nutné data zakódovat. Nejčastěji se používá metoda **BER** (**B**asic **E**ncoding **R**ules).

b) **X.500 –** pro svou těžkopádnost se příliš nepoužívá
   - série protokolů pro počítačové sítě, které definují službu elektronického adresáře. Architektura tohoto protokolu je postavena na bázi KLIENT – SERVER. Komunikuje přes OSI model.

c) **Lightweight Directory Access Protocol (LDAP)**
   - přehled klientských a serverových aplikací (Tab. 1 a Tab. 2)

d) **Active Directory**

e) **Kerberos**
   - síťový autentizační protokol, na bázi tiketů a symetrické kryptografie, který umožňuje v nezabezpečené síti bezpečně identifikovat uživatele.

Tab. 1. Seznam klientských LDAP aplikací[4]

Název aplikace	Platformy
LDAP Admin	Open source, MS Windows
LDAP Manager	MS Windows
LDAP Account Manager	Pro více platforem - PHP GNU, GPL
PhpLDAPadmin	Pro více platforem – PHP GNU, GPL
Kontakt KAddressBook	Linux / Unix
Evolution	Linux / Unix
Apache Directory Studio	Open source pro více platforem
Fusion Directory	Pro více platforem – GNU GPL, PHP, Web
Active Directory Explorer	MS Windows
JXplorer	Pro více platforem – Open source, Java
RoundCube	Pro více platforem – GNU GPL, PHP

[4] Vlastní tvorba podle článku "List of LDAP software". [6]

Directory Utility	Mac OS X
Address Book	Mac OS X

Tab. 2. Seznam serverových LDAP aplikací[5]

Název	Autor
Open LDAP	Kurt Zeilenga
Active Directory	Microsoft
Oracle Directory Server - Enterprise Edition	Oracle
Apache Directory Server	Apache Software Foundation
Apple Open DIrectory	Apple Inc.
IBM Tivoli Directory Server	IBM
Novell eDirectory	Novell
Virtual Identity Server	Optimal IdM
FreeIPA	Red Hat

1.3 Problematika řízení přístupů do IT systémů

V současnosti neustále roste tlak na efektivnost a kvalitu IT programů a služeb. Stoupají nároky na správu uživatelů. Naproti tomu je znatelný tlak na snížení potřebných pracovníků, kteří tuto práci vykonávají. Tuto problematiku efektivně řeší nasazení IdM, který umožnuje zautomatizování procesu vytváření účtů a změn hesel. Zároveň umožnuje ucelený pohled na všechny uživatele systému dané společnosti. Implementace IdM je nutností u společností s více zaměstnanci, např. průmysl, státní správa, telekomunikace, finanční sektor apod.

Vedení společnosti ocení úsporu nákladů na přístupová oprávnění, snížení počtu pracovníků na správu, snížení nákladů na školení uživatelů při zavádění nových systémů, snížení rizik zneužití, splnění auditních požadavků na bezpečnost dat a v poslední řadě také plné zautomatizování HR procesů spojených s nástupem a odchodem pracovníků atd.

[5] Vlastní tvorba na základě článku “List of LDAP software”. [6]

2 SPRÁVA IDENTIT V MENŠÍCH SPOLEČNOSTECH

2.1 Active Directory

Služba Active Directory (AD) [7] byla představena poprvé s operačním systémem MS Windows 2000 server jako přímý nástupce Domény Windows, která používala stromovou strukturu adresáře pro uchování informací.

AD realizuje adresářové služby LDAP. Zahrnuje řadu funkcí, mezi něž patří poskytování centrálních služeb pro autentizace i autorizaci a správu uživatelských účtů.

AD tvoří LDAP, Kerberos a DNS. [8]

Pro správnou funkci AD je potřeba fungující DNS server, pomocí kterého si stanice zjišťují umístění služeb v síti (Kerberos, LDAP atd.).

AD obsahuje informace o uživatelích, PC, tiskárnách, sdílených složkách a můžeme ji přirovnat k telefonnímu seznamu.

Všechny objekty (pracovní stanice, uživatelé) jsou tříděny do logických hierarchických skupin, které jsou používány k autentizaci uživatelů a zdrojů ve firemní síti.

Pracovní stanice AD je individuální PC/server v síti, má unikátní účet, který umožňuje autorizaci a ověření pro přístup k doménovým zdrojům.

Server může být **Doménový řadič** (**DC**) nebo **Globální katalog** (**GC**).

- **Doménový řadič** je AD server, který autentizuje uživatele a může udržovat pouze jednu doménu.
- **Globální katalog** je centrální uložiště, které obsahuje informace o objektech z celého stromu nebo lesa. Může být provozován pouze na serveru DC.

AD služby se vžily hlavně díky několika klíčovým vlastnostem:

- škálovatelnost ve velkém měřítku (tisíce uživatelů v jedné doméně).
- rychlý a efektivní hledací mechanismus.
- objekty mohou být umístěny kdekoliv, ale stále budou mít bezpečný přístup k doméně či síti.
- velký stupeň bezpečnosti díky vrstvenému zabezpečení, které používá politiky a oprávnění.
- centralizované uložiště, které umožňuje obnovu a zálohování rychle a efektivně
- centralizovaný management služeb.
- umožňuje **SSO** (**S**ingle **S**ign-**O**n) a přihlašovací skripty.
- individuální profily.
- povinné profily.
- centralizovaný Audit.

Nástroje pro správu AD [9]

- **ADUC** (**A**ctive **D**irectory **U**sers and **C**omputers) umožňuje provést změny vlastností u několika uživatelských účtů najednou, které se nacházejí v jedné OU (**O**rganization **U**nit). Možné je použít i funkci vyhledávání.
- **Nástroje příkazové řádky (CMD)** - vztahují se k nim nástroje **dsmod, dsadd** a **drm**, které mohou spravovat pracovní stanice, účty uživatelů atd. v AD.
- **CSVDE** - importuje a exportuje data z AD do souboru ve formátu .CSV.
- **LDIFDE** – vytváří, odstraňuje a mění objekty adresářů v operačních systémech MS Windows XP Professional a MS Windows server 2003. Pomocí této služby lze přidat do AD data z jiných adresářových služeb a zároveň je exportovat.
- **Powershell** - shell se skriptovacím jazykem umožňuje spravovat a konfigurovat systém pomocí 130 nástrojů příkazového řádku. Pro chod potřebuje **.Net Framework 2.0** a vyšší.

Objekty AD

Objekty jsou fyzické entity v síti, které mohou být popsány jako skupina atributů.

Objekty mohou být uživatelé, terminály, tiskárny, sdílené složky apod., které se sdružují na logické úrovni do organizačních jednotek **OU**. OU s objekty tvoří domény a v AD jsou označovány jako kontejnery, ty se používají pro seskupování objektů do logických administračních skupin, na které můžeme delegovat administrační oprávnění.

Doména

Doména je skupina počítačů sdílejících společnou adresářovou databázi. Názvy domén musí být jedinečné a každá doména má své vlastní zásady zabezpečení a určitý vztah důvěryhodnosti k ostatním doménám. Neexistuje žádný limit objektů, které může doména obsahovat a může se skládat z více sítí a podsítí.

Objekty nemusí být na stejném fyzickém místě. V adresářové databázi domény jsou současně objekty určující účty uživatelů, skupin, počítačů a sdílené prostředky (složky, tiskárny atd.).

Doménový strom

Množina názvů, ve které je každý název odvozen z jediného názvu kořene.

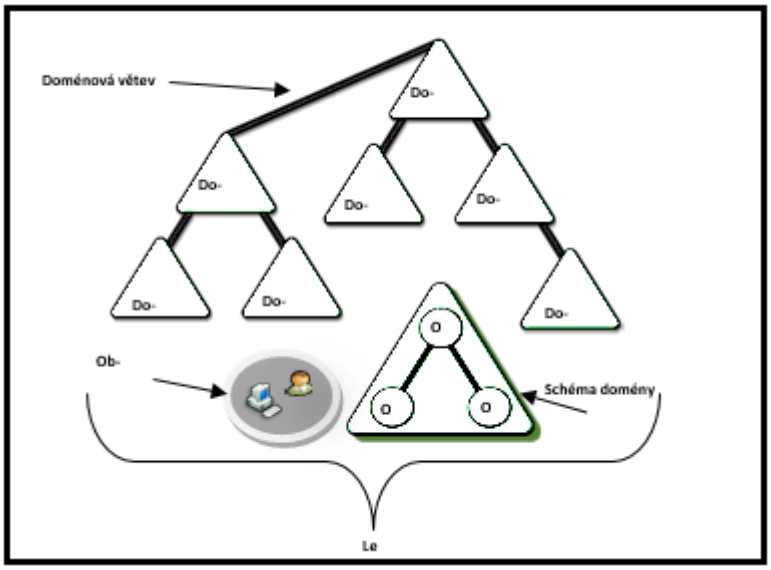
Doménový řadič je nejvyšší autorita, která je zodpovědná za všechny autentifikace, autorizace, vymazání, modifikace uvnitř domény. Pokud má uživatel přístup do určité domény, může se do ní přihlásit z jakékoliv pracovní stanice, která je součástí této domény.

Přístupy a práva mohou být nastaveny na všechny objekty v doméně nebo na individuální úrovni.

Doménový les (Forest)

Skupina doménových stromů.

Nejvyšší úroveň bezpečnostního větvení obsahuje objekty jako domény, uživatelé, pracovní stanice, ostatní síťové zdroje a tiskárny. Výměna informací a dat může proběhnout pouze mezi objekty uvnitř lesa a obsahovat jednu i více domén a kombinovat je do lesa.



Obr. 3. AD - Logická struktura[6]

Znaky AD – domény:

- Hierarchická struktura kontejnerů a objektů.
- Unikátní jméno domény.
- Bezpečnostní mechanizmus, který autentizuje a autorizuje přístup ke zdrojům domény.
- Zásady/politiky, které umožňují nebo zakazují přístup uživatelů, pracovních stanic k doméně.
- Organizační jednotky se zobrazují pouze v doméně a mohou označovat určité pracoviště, místo, skupinu atd., a také obsahují informace o ostatních objektech, jako jsou uživatelé, kontakty, sdílené složky atd.
- Organizační jednotka může obsahovat další organizační jednotku a ty jsou propojeny uvnitř jedné domény.
- Skupinové zásady/politika může být nastavena na úrovni organizační jednotky.

[6] Vlastní tvorba na základě článku “Active Directory Architecture”. [8]

Organizační jednotka

Organizační jednotkou je označen např. uživatel, určitá skupina a pracovní stanice uvnitř domény.

Uživatel AD má unikátní identitu a **SID** (**S**ecurity **Id**entifier). Jeho účet je unikátní a zabezpečený heslem. Pro správu uživatelů můžeme použít **ADUC** (**A**ctive **D**irectory **U**sers and **C**omputers).

Skupina

Obsahuje uživatele a pracovní stanice, které jsou součástí určité skupiny, kde se autorizace, povolení a restrikce aplikují na všechny členy skupiny.

Třídění skupin podle zaměření

- zabezpečené skupiny
- distribuční skupiny

Podle rozsahu:

- **Lokální skupiny**, které dávají přístup ke zdrojům ve stejné doméně jako je skupina a uživatel může být z jiné domény.
- **Globální skupiny**, které dávají přístup ke zdrojům v různých doménách uživatelům ze specifické domény.
- **Univerzální skupiny** - uživatelé mají přístup ke zdrojům z jiných domén.

Kontakt

Kdokoli, kdo není součástí organizace, ale má nějaké propojení s ní (dodavatel, zákazník) na rozdíl od interního uživatele, se nemůže přihlásit do sítě nebo přistupovat ke zdrojům v doméně a ani mu nemůže být přidělena autorizace, restrikce nebo přístupy.

Objekty jsou identifikovány jejich atributy (jméno, místo, oddělení).

Jméno: Uživatel

Místo: Workgroups/uživatel

Oddělení: IT

Každý objekt může být autentizován a mohou mu být přidělena práva.

Identifikátory domény:

- **GUID** - unikátní identifikátor objektu

- **SID** - unikátní identifikátor uživatele, který se používá pro Kerberos a zařazování do skupin.

Zásady skupin (GPO)

Pravidla aplikovaná v podniku.

- nastavení zásad skupin – umožňuje řídit konfiguraci OS a jeho komponent
    a) Nastavení softwaru (automatická instalace a upgrade).
    b) Nastavení systému Windows (nastavení a ovládaní klíčových vlastností systému).
    c) Šablony pro správu (slouží ke změnám konfigurací OS – komponentů Windows a aplikací).

Předvolby zásad skupin

a) Nastavení OS, konfigurace klíčových skupin a registrů.
b) Konfigurace ovládacích panelů, aplikace spočívá ve vazbě GPO na součásti AD DS (lokality/sítě, domény a organizační jednotky).

2.2 Ochrana a bezpečnost informací v AD

Komplexní opatření proti hrozbám v IS/ICT je implementace kryptologie[7]. Kryptologie je základním postupem pro zajištění důvěrnosti dat při jejich ukládání a přenosu po nechráněných kanálech. Vedle kryptologie je velmi dynamicky se rozvíjející součástí informační bezpečnosti biometrie. Dalším bezpečnostním opatřením je politika – tj. přidělení odpovědnosti za bezpečnost.

2.3 Význam bezpečnosti IS/ICT[8]

Softwarové systémy zpracovávají informace a data, která mají pro firmy velkou hodnotu.

Bez zabezpečení lze se současnými prostředky ICT významná data získat, změnit nebo zničit. Bezpečnostní opatření by měla tvořit nezbytnou součást každého softwarového systému.

Mezi základní možnosti bezpečnostní hrozby patří:

- **Škodlivý software** (počítačové viry, trojské koně, síťové červy, Spyware atd.).
- **Počítačová infiltrace** (neautorizovaný vstup do IS, do jeho programu a paměti, jeho prostřednictvím se šíří vlastnosti škodlivého softwaru a útoky hackerů).
- **Pasivní odposlech** (neautorizované monitorování nebo zaznamenání dat přenášených komunikačním kanálem – internetem, firemní síti).

Základním protiopatřením proti těmto hrozbám je ochrana, kterou zabezpečuje legislativa, hardware a software (antivirové programy, firewally apod.), pravidelný update OS.

Dalším opatřením je využívání potenciálu **autentizace a autorizace** (znalost hesla, kryptografické klíče pro digitální podpis), **tokeny** - čipové a magnetické karty apod., **dva typy biometrie** – fyziologická a behaviorální a **kombinace výše uvedených postupů**.

---

[7] Kryptologie je matematický obor zabývající se kryptografií a kryptoanalýzou.

[8] ČECH, Pavel, Vladimír BUREŠ a Melissa. CRAFT. Podniková informatika: planning, implementing, and maintaining a Microsoft Windows Server 2003 Active Directory infrastucture : self-paced training kit. [10]

Dalším opatřením je zálohování dat (off-line/on-line, cluster, Cloud, zdvojení center zpracování, RAID pole atd.), které minimalizuje dopady případného poškození dat.

Zamezení možnosti zjištění informačního obsahu neoprávněným osobám zajišťuje používání šifrování – kryptografie.

Prakticky je nutné plánovat a řídit bezpečnostní opatření a používat je ve vhodné kombinaci, jedná se o bezpečnostní politiku, která ve firmě stanoví povinnosti a odpovědnost na dodržování bezpečnostních opatření.

2.4 Kryptologie

Kryptologie je matematický obor zabývající se **kryptografií** a **kryptoanalýzou**. Kryptografie je věda o utajování zpráv a kryptoanalýza je věda o jejím dekódování. Moderní kryptografie se uplatňuje např. při potvrzení integrity zprávy a autentizaci uživatelů.

Existují dva druhy:

- **Pseudojednosměrná** - základní postup je šifrování
- **Jednosměrná** – hash

Podle druhu klíče se kryptologie dělí na **symetrickou** (tajný klíč) a **asymetrickou** (veřejný a tajný klíč).

Symetrické šifrování zajišťují šifrovací algoritmy, které zprávu zašifrují a dekódují pomocí jednoho klíče, odesilatel a příjemce musí mít k dispozici tajný klíč. Příkladem symetrických algoritmů je **DES** (**D**ata **E**ncryption **S**tandard), **AES** (**A**dvance **E**nryption **S**tandard), **IDEA** (**I**nternation **D**ata **E**nryption **A**lgoritm), **Blowfish** a jeho nástupci **Twofish** a **Threefish** (u kterých není známo efektivní prolomení) a **Serpent** aj.

DES vyvinula firma IBM v únoru 1975. Zpráva se rozdělí do bloků o velikosti 64 bitů a každý blok se rozdělí na 2 části, které se kombinují s klíčem, 16x dohromady. Operaci šifrování zajištuje jeden blok 64 bitového otevřeného textu na blok 64 bitového zašifrovaného textu. Pro šifrování se používá klíč o velikosti 56 bitů.

Algoritmus využívá dvou kryptografických technik - substituce a permutace.

AES je mezinárodní standard, který byl udělen symetrické blokové šifře **Rijndael**, která vychází z kryptosystému **Square** a mezi její hlavní výhody patří jednoduchá hardwarová a softwarová implementace a rychlost.

IDEA je symetrická bloková šifra, která byla používaná v PGP a má volitelný algoritmus v OpenPGP. Pracuje po 64 bitových blocích za použití 128 bitového klíče, skládá se z 8 identických transformací. Je odolná vůči diferenční kryptoanalýze a v současné době neexistuje žádné proražení této šifry.

Blowfish je symetrická bloková šifra, navržena v roce 1993 B. Schneierem. Jedná se o Open-source a je používaná v mnoha systémech. Blowfish poskytuje rychlé šifrování a dodnes není známa metoda jejího prolomení. Schneier navrhl Blowfish jako alternativu k zastarávajícímu DES.

Asymetrické šifrování používá dva klíče. Jeden klíč je privátní a druhý veřejný. Jestliže chceme zaslat tajnou zprávu, použijeme veřejný klíč a zašifrujeme text zprávy. Ta se dá dekódovat privátním klíčem příjemce. Nejznámější asymetrický algoritmus je **RSA**.

RSA je šifra s veřejným klíčem, která byla vytvořena v roce 1977 a je založena na využití prvočísel a faktorizace, která se považuje za skoro neřešitelný problém. Klíče jsou dlouhé v rozmezí 1024-2048 bitů. S délkou klíče stoupá obtížnost prolomení šifry. Plné dešifrování je nepravděpodobné.

Symetrické šifrování je jednoduché a rychlé, ale neřeší ověřování identity.

Asymetrické šifry jsou časově náročnější, ale bezpečnější.

2.5 Zásady ochrany IS[9]

Základním cílem ochrany IS je minimalizovat souhrn všech rizik. Koncepci bezpečnosti IS tvoří legislativa administrativní kontroly, fyzická ochrana a kontroly bezpečnosti zabudované v systému. Mezi základní opatření plánovaného bezpečnostního opatření patří:

- Politika (přidělení odpovědnosti za bezpečnost).
- Současný stav (riziková analýza).
- Doporučení (realizovatelnost bezpečnostního opatření).
- Odpovědnost (seznam pracovníků s odpovědnostmi, úkoly a finanční hodnocení).
- Časový harmonogram (zavádění bezpečnostních opatření do praxe).
- Sledování (vyhodnocení bezpečnostní politiky).

Riziková analýza [12]:

- Vymezení hodnot systému.
- Stanovení zranitelnosti hodnot systému.
- Odhad pravděpodobnosti zneužití zranitelných míst.
- Výpočet odhadu ztrát.
- Výčet použitelných bezpečnostních opatření a jejich ceny.
- Plán úspor v důsledku zavedení bezpečnostních opatření.

Nejznámější normy pro informační bezpečnost

- **COBIT** (**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology) [13] - mezinárodní standard pro správu a řízení informatiky. Soubor praktik, které umožňují dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik.

[9] GALBA, Alexander a Antonín PAVLÍČEK. Moderní informatika. [11]

- **ITIL (I**nformation **T**echnology **I**nfrastructure **L**ibrary) - soubor postupů zaměřující se na využívání a zkvalitňování informačních technologií (IT), jak ze strany dodavatelů IT služeb, tak i z pohledu zákazníků.
- **ISO/IEC 27002** – mezinárodní bezpečnostní standard zaměřující se na bezpečnost.

2.6 Digitální podpis

V České republice je digitální podpis zakotven v zákoně č. 227/2000 Sb.

Zde se popisuje, že se jedná o údaj v elektronické podobě, který je připojen k datové zprávě a slouží jako metoda k jednoznačnému ověření identity podepsané osoby. Vyšší formou elektronického podpisu je **zaručený elektronický podpis** (§ 2 písm. b).

Elektronický podpis vychází z asymetrického šifrování.

Certifikáty a certifikační autority

Vhodné řešení pro zamezení falzifikátů je využití třetí osoby, které budou důvěřovat jak příjemce, tak odesilatel. Pro tento účel slouží tzv. certifikační autority (poskytovatelé certifikačních služeb) a bezpečnostní certifikáty (certifikáty). Certifikační autorita je nezávislý subjekt, který provádí ověřování identity jiných subjektů a vydávání certifikátů (certifikační služby). Certifikát spojuje určitou identitu s veřejným klíčem, k němu je potřeba připojit doplňující informace. Základní obsah certifikátu je tvořen následujícími údaji:

- Jedinečné sériové číslo.
- Vydavatel.
- Identifikace vlastníka.
- Algoritmus podpisu – Hash / RSA / DSA.
- Veřejný klíč / privátní klíč.
- Podpis vystavitele aj.

2.7 Biometrie

Je věda o využívání fyziologických a behaviorálních (chování) charakteristik lidí pro jejich rozpoznávání, identifikaci a verifikaci. V praxi se využívají unikátní charakteristické rysy

člověka (oční sítnice, geometrie ruky, hlas nebo otisk prstu atd.), které jsou převáděny do IS.

Základní požadavky pro biometrii:

- Jednoduchost.
- Zachování tajemství.
- Věrohodnost.
- Uživatel (nesmí být vystaven zdravotnímu riziku).

Aplikace biometrického systému musí akceptovat stárnutí osob a změny biometrických charakteristik.

Jednotlivé biometrické technologie [14]

- **Geometrie ruky** [15] – v roce 1996 byl tento systém použit pro identifikace na OH v Atlantě. Aplikace v praxi je omezená pro její nepřesnost. V USA je systém normalizován – ANSI INCITS 396-2005.
- **Geometrie tváře** – založena na srovnávání obrazu s obrazem, který je uložen v centrální databázi. V současné době existuje několik technik rozpoznávání tváři. Nejpoužívanější je **metoda geometrických vlastností** a **metoda porovnávání šablon.**
- **Duhovka oka** – k této metodě je potřeba kvalitní digitální kamera a dobré infračervené osvětlení oka.
- **Sítnice oka** – pro získání obrazu se používá zdroj světla s nízkou intenzitou záření – Opto-elektrický systém (červená LED dioda). Tato metoda je nepříjemná pro uživatele.
- **Verifikace podle způsobu pohybu očí.**
- **Verifikace pomocí povrchové topografie očí.**
- **Struktura žil na zápěstí** – technologie spočívá ve snímání hřbetu ruky speciální kamerou při infračerveném osvícení.
- **Verifikace podle článku prstu.**
- **Verifikace podle vrásnění článku prstů.**

Behaviometrika [14]

- **Psaní na klávesnici** – technologie je obdobou dynamického podpisu. Sleduje dynamiku úhozů na klávesnici, která se u různých lidí liší.
- **Dynamika podpisu** – metoda, která využívá kombinaci anatomických a behaviorálních vlastností člověka při podpisu.
- **Dynamika chůze.**
- **Otisk prstu** – nejpoužívanější biometrická metoda (u přenosných počítačů Business třídy) a v současné době i možnost čtení otisku prstu pomocí mobilního zařízení.
- **Akustická charakteristika hlasu.**
- **Verifikace podle pachu.**
- **Verifikace podle DNA** – struktura DNA je odlišná u všech lidí s výjimkou jednovaječných dvojčat a nemění se s věkem.
- **Biometrie ušního boltce.**
- **Verifikace odrazem zvuku v ušním kanálku** – nová metoda, která není v současné době rozšířená**.**
- **Verifikace podle tvaru a pohybu rtů.**
- **Identifikace podle rýhovaní nehtů.**
- **Identifikace podle spektroskopie kůže.**
- A další **(**indikace podle bioelektrického pole uživatele, zubů atd.).

Přestože biometrické metody vykazují v laboratořích dobré výsledky, v praktickém využití mohou nastat komplikace, proto jsou dále vylepšovány.

3 SPRÁVA IDENTIT VE VĚTŠÍCH SPOLEČNOSTECH

LDAP – protokol vytvořený pro přístup k datům na adresářovém serveru DS.

Protokol LDAP vychází z DAP. Byl vytvořen X.500.

3.1 LDAP servery

Podnikové počítačové sítě s velkým množstvím síťových komponent, aplikací a uživatelů, vyžadují IS založený na datech, obsahujících jména, adresy a další informace o subjektech a objektech zahrnutých ke komunikaci. K tomu slouží adresář databáze, který je označován jako **DIB**. DIB se skládá ze záznamu o objektu, který je identifikován atributy, které mohou být definovány různými hodnotami. DIP a jeho struktura je definování **ITU-T rec. X.501**.

Informace uložené v DIB mají danou strukturu a hierarchii využívající stromovou strukturu. Je reprezentován jako **D**irectory **I**nformation **T**ree (**DIT**).

Bezpečnost LDAP [16]

Důležitá data uložená v adresářovém serveru je nutno chránit a proto součástí LDAP je bezpečnostní politika. Bezpečnostní model je popsán např. v dokumentech RFC 2829.

Tento model definuje základní hrozby pro LDAP:

- Neautorizovaný přístup přes data-fetching
- Neautorizovaný přístup k informacím získaných sledováním cizích přístupů
- Neautorizovaná změna dat a konfigurace
- Nadměrné neautorizované využití zdrojů – **DoS** (**D**enial **o**f **S**ervice)

Ověřování LDAP v3:

- **Základní ověření**
  Uskutečňuje se na znalosti DN (**D**istinguished **N**ames) a hesla, data jsou přenášena v textovém formátu nebo šifrována pomocí **Base64**.

- **Ověření pomocí PKI**
  Klient digitálně podepíše náhodně vygenerovaný řetězec dat a pošle je spolu s certifikátem na server. Zde se ověří certifikát s certifikátem uloženým na serveru.
- **Jednoduché ověření s použitím SASL (S**imple **A**uthentication and **Se**curity **L**ayer)
  SASL je Framework zásuvných modulů pro použití alternativních bezpečnostních mechanismů (Kerberos V4, TLS atd.).
- **Bez ověření** (anonymní přístup)
  Slouží pro přístup do adresáře bez poskytnutí ověřovacích informací. Administrátor může nastavit přístup do adresáře dle vlastního uvážení. Lze zabezpečit přístup k určitému typu dat, obsahující např. informace o kontaktech (telefonní čísla, e-maily apod.)
- **ACI** (**A**ccess **C**ontrol **I**nsructions).
  Při použití ACI se může řídit přístup k celému adresáři, stromu, části stromu, jednotlivým záznamům. Práva lze nastavit pro jednotlivé uživatele, skupinu uživatelů i pro klienty s určitou IP adresou nebo doménovým jménem.

3.2 Řešení LDAP

a) Apache Directory Server [17]

ADS je malý škálovatelný LDAP server, který je vyvinut jako open-source pod záštitou Apache Software Foundation, založený na jazyce Java a je možno toto řešení používat v jiných projektech založených na prostředí Java. Např. **Sun web Server**, **GlassFish**, **Oracle Application Server**. Toto řešení lze nainstalovat na operačních systémech **Sun Solaris**, **OpenSolaris**, **Microsoft Windows**, **Red hat Linux**, **H**ewlett **P**ackard **U**ni**X**. Apache Directory Server se často v praxi nasazuje díky svým unikátním zásuvným modulům, dále možnosti vytvářet virtuální adresáře, proxy a brány.

b) Red Hat Directory Server [18]

Řešení, které centralizuje uživatelské profily, nastavení, politiky a kontrolu přístupů do síťového registru. Komerční řešení je součástí Red Hat Enterpise Linux a otevřené řešení je dostupné pod licencí GPL s názvem **389 Directory Server**. Mezi jeho hlavní vlastnosti

patří implementace LDAP verze 2 a 3, logické rozdělení adresáře na několik serverů, centralizovaná správa uživatelů a jejich profilů, centrální repositář pro uživatelské profily a nastavení, možnosti Single-Sign on, možnost lineárního rozšíření počtu CPU.

c) Novell eDirectory [19]

Je to multiplatformní otevřené řešení, které je možné použít v operačních systémech **Sun Solaris**, **Microsoft Windows**, **SUSE Linux**, **Red Hat Linux, H**ewlett **P**ackard **U**niX.

Vychází z produktu společnosti Novell – Novell Directory Services, který je založen na standardu X.500 a umožňuje realizovat centrální správu heterogenních sítí (HetNets).

d) **OpenLDAP** [20]

Volně šiřitelná implementace protokolu LDAP, který je uvolněn pod BSD licencí nazývanou OpenLDAP public Licence. Řešení je dostupné pro celou škálu operačních systému – **Sun Solaris**, **OpenSolaris**, **Microsoft Windows**, **Red hat Linux**, **H**ewlett **P**ackard **U**ni**X**, **Android**, **Mac OS X**. Nevýhodou toho řešení je nutnost restartu adresářového serveru v případě změny konfiguračních parametrů.

e) Sun Directory Server

Výkonný adresářový server, který poskytuje základní adresářové služby a velké množství doplňkových datových služeb. Obsahuje LDAP adresářové služby, proxy server s load-balacing, virtualizaci a další. Je možné ho propojit s MS AD a synchronizovat identity, hesla atd. Podporuje operační systémy **Sun Solaris**, **OpenSolaris**, **Microsoft Windows**, **Red hat Linux**, **H**ewlett **P**ackard **U**ni**X.** Adresářový server má 64 bit adresářový systém třídy enterprise. V prostředí s velkým množstvím dat je nutné rozdělení na více serverů. Sun Java Systém Directory Server Enterprise nabízí možnost integrace pro konsolidaci dat.

Sun Java Systém Directory Server Enterprise podporuje operační systémy **Sun Solaris**, **OpenSolaris**, **Microsoft Windows**, **Red hat Linux**, **H**ewlett **P**ackard **U**ni**X, Ubuntu GNU Linux** a **IBM AIX**. Toto řešení podporuje databáze pro virtualizace - **MySQL 5.0, Oracle 9i** a **10g** a **IBM DB2**. **Sun Java Systém Directory Server Enterprise** obsahuje virtuální adresář a službu virtuálního proxy serveru a mezi jeho klíčové vlastnosti patří centralizovaný repositář pro identity, služby adresářového proxy serveru, neomezený počet master serverů,

editor objektů na web rozhrání, centralizovaná správa globálního adresáře, sjednocený pohled na identity a virtuální adresáře.

OpenDS

Open-source projekt, dostupný pod licencí CDDL, založený na řešení Sun Directory Server.

Umožňuje vytvářet standardizované adresářové služby pro internetové aplikace, zahrnuje vysoce propustné webové sítě jako kalendář, email atd. Podporuje operační systémy **Sun Solaris**, **OpenSolaris**, **Microsoft Windows**, **Red hat Linux**, **H**ewlett **P**ackard **U**ni**X, Ubuntu GNU Linux** a **IBM AIX**.

OpenDS – adresářový Java server má volně šiřitelný software pod licencí CDDL. Software OpenDS je navržený pro výkon a škálovatelnost, využívá horizontální strukturu dat. Umožnuje přírůstkové zálohování, komprimaci, šifrování, elektronický podpis, ověření a on-line obnovení vedoucí k vyšší spolehlivosti dat. Aktuální stabilní verze 2.2 Update 1 je z roku 2010. OpenDS je klíčovým prvkem produktů IDN společnosti Sun.

Mezi hlavní vlastnosti patří implementace LDAP V3, která je založená kompletně na Java technologiích. Další vlastností je rozšířená replikace, politika správy hesel a podpora zálohování a obnovy dat, jednoduchá instalace a integrace do jiných produktů.

Oracle Directory Services

Toto řešení poskytuje služby, které nabízí řešení virtualizace, úložiště a synchronizace adresářových dat. Implementace služeb LDAP na technologii databáze Oracle může poskytnout značnou úroveň rozšiřitelnosti, vysokou dostupnost a bezpečnost uložených dat.

Oracle Internet Directory umožňuje podporu velkého množství internetových aplikací.

Oracle Virtual Directory je virtualizační službou. Je to systém, který poskytuje jednotný pohled na různé služby uvnitř organizace.

IBM Tivoli Directory Server [21] je další implementací LDAP adresářového serveru. Je součástí skupiny produktů IBM Tivoli Identity and Access Management. Poskytuje proxy server umožňující další rozšíření pro správu systému pomocí webového administračního nástroje.

Microsoft Active Directory [7] je kombinace několika síťových služeb zahrnující adresářový server založený na LDAP, ověření Kerberos a systému DNS. Poskytuje centralizovanou správu sítě. AD je logické seskupení uživatelů, počítačů v doméně a dalších entit, centrálně spravované servery (**D**omain **C**ontroller). Zdroje mohou být například tiskárny, služby, web, e-mail, FTP, uživatelé (uživatelská konta, skupiny a počítače). AD může udržovat objekty v několika úrovních. Vrcholem hierarchické skupiny je les (forest), dalšími logickými částmi je strom (tree) a doména. Adresářový systém je nepřenosný na jiné OS nebo HW.

Předností je možnost využití LDAP serverů a uložených identit jako zdroj dat pro další aplikace a služby. Tyto servery je možno integrovat s OS aplikačními servery sloužící pro poskytování obsahu v rámci intranetu a extranetu.

4 ANALÝZA PŘÍSTUPU A SPRÁVY IDENTIT

Kapitola se zabývá analýzou modelové organizace při použití vhodného **RBAC** (**R**ole-**B**ased **A**ccess **C**ontrol) modelu a vytvořením fiktivní firmy.

4.1 Modelová organizace

Analyzovaná organizace je firma, která vznikla v roce 2010 a její specialisté poskytují komplexní služby v oblasti vývoje softwaru a informačních systémů na domácích trzích. Jedná se o malou firmu, která má 30 zaměstnanců, její růst je dynamický. Sídlo firmy je v ČR.

Úložištěm uživatelů je OpenLDAP a používá HR systém Pohoda.

Pro tuto organizaci má význam aplikace REDMINE.

Vlastnosti této aplikace: [22]

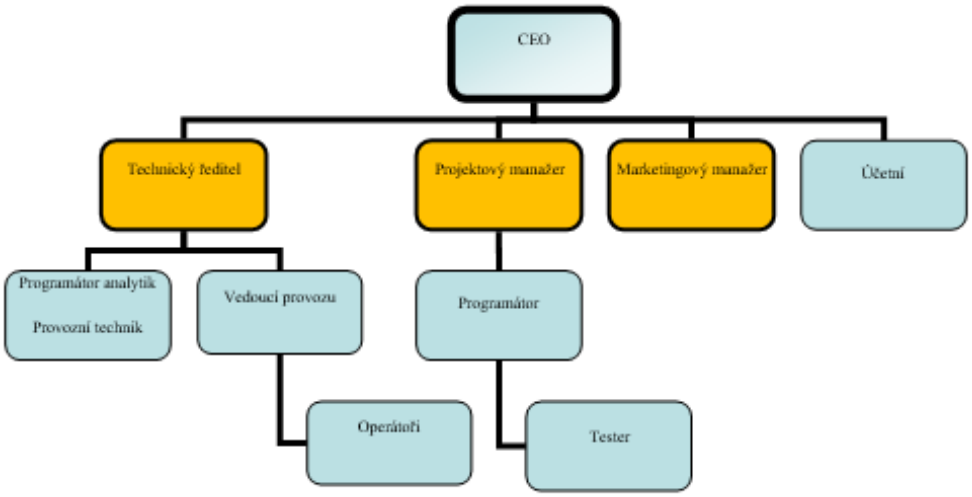
- Autentizace uživatelů probíhá prostřednictvím LDAP.
- Autorizace uživatelů na základě přiřazených skupin.
- Skupiny jsou přiřazovány uživatelům podle potřeby.
- Podpora více projektů.
- Flexibilní systém řízení přístupů založený na rolích.
- Flexibilní systém pro správu úkolů.
- Ganttův diagram[10] a kalendář.
- Správa dokumentů a souborů.
- Oznámení pomocí emailu a zdrojů (feeds).
- Wiki pro každý projekt.
- Fórum pro každý projekt.
- Snadné sledování času u jednotlivých projektů.

[10] Ganttův diagram se využívá při řízení projektů pro grafické znázornění naplánování posloupnosti činností v čase. V základní podobě neobsahuje vztahy mezi činnostmi, ale moderní softwarové nástroje pro plánování projektů do něj tyto závislosti obvykle přidávají. [23]

- Uživatelská pole pro úkoly, časové vstupy, projekty a uživatele.
- Integrace SCM (SVN, CVS, Git, Mercurial, Bazaar a Darcs).
- Podpora vícenásobné LDAP autentizace.
- Uživatelé se mohou sami registrovat do systému.
- Podpora více jazyků.
- Podpora více databází.
- Podpora pluginů.

U organizace se vyskytují vztahy nadřízený a podřízený.

Organizace má následující organizační strukturu:



Obr. 4. Organizační struktura podniku

Řízení přístupu uživatelů ke zdrojům je nejčastěji prováděno na základě přiřazených skupin. V oblasti používaných uložišť mají značný podíl LDAP implementace.

Snadná správa identit a přístupu

Snadnou správu identit a přístupů zabezpečí těchto 10 kroků: [24]

- Vytvoření skladu identit, který bude obsahovat přístupová práva stávajících uživatelů a provedení federalizace hesel pomocí adresářových služeb pro snížení manuálního zadávání.

- Vytvoření sady pro správu rolí podniku a definování přístupových práv uživatelů zadáním specifických rolí tak, aby se dostali pouze k potřebným prostředkům.
- Definování rolí pomocí podnikových termínů pro snadnou srozumitelnost.
- Manažeři musí potvrdit, že oprávnění k aplikacím stanovená pomocí pravidel jsou správná.
- Vytvoření podnikových rolí, které je možno použít pro celou firmu.
- Použít další schvalovací proces pro celopodnikové role.
- Přizpůsobit systém žádostí tak, aby obsahoval podnikové role.
- Oddělit role tak, aby uživatel nemohl mít více než jednu roli.
- Použít IAM i pro obchodní partnery a zákazníky.

Řízení přístupu

Řízení přístupu je jednou ze základních součástí IdM. Z technologického hlediska lze využívat tyto služby

Autentizace

Proces ověření identity subjektu

Více faktorová identifikace

Spojení více faktorů pro autentizaci např. heslo, karta, klíč nebo biometrické údaje v různé kombinaci.

Autorizace

Proces udělení práv subjektu pro vykonávání aktivit v systému.

Seznam pro řízení přístupu (ACL)

Určuje jaká entita má povolení přistupovat k zabezpečenému objektu a jaké operace s ním může provádět.

Jednotné přihlášení (SSO)

Uživatel zadává přihlašovací údaje pouze jednou. Například pomocí čipových karet, tokenů, Kerberos atd.

Jednotné webové přihlášení (Web SSO)

Varianta SSO. Poskytovatel předá webové stránce informace o autentizaci a autorizaci uživatele. Např. Facebook connect, OpenID, atd.

Řízení přístupu na základně RBAC

Přístup na základě rolí.

Řízení přístupu na základě ABAC (Attribute based access control)

Řízení na základě atributů identity. Podmínky, které musí uživatel splňovat pro přístup, jsou předem stanovené.

Diskrétní řízení přístupu (DAC)

Vlastník (administrátor) sám určí, kdo má oprávnění se zdrojem nakládat a s jakými privilegii.

Povinné řízení přístupů (MAC)

Systém udělí přístup ke zdroji jen tehdy, pokud existuje pravidlo. Používá se pouze u velmi citlivých informací kvůli náročné administraci.

Služba pro bezpečné tokeny

Vydává bezpečnostní tokeny.

4.1.1 Systém řízení identit

- **Řízení životního cyklu identit**

V této části systému jsou zahrnuty funkce pro správu identit a informace o nich. Mezi tyto informace patří např. identifikátory, identifikační informace a jejich atributy. Jsou zde i registrační postupy spojené s vydáním identifikačních údajů.

- **Registrace a ověření totožnosti uživatele**

Prvním krokem registrace uživatele je vznik jeho identity v systému. Identita je vyjádřením určité entity, jejíž vznik je rozdílný podle pravidel společnosti a typu entity. Druhým krokem je identifikace entity a její ověření/zaregistrování do systému.

- **Práva atributů**

Atributy identit jsou prostředky pro uchování dat související s identitou. Těmito daty mohou být osobní informace – telefonní číslo, jméno, provozní informace (informace o doméně, IP adresy atd.), informace související se zaměstnáním (pozice, číslo kanceláře atd.), informace související se systémem pro řízení identit (oprávnění, role, zákazy apod.). Je třeba mít definované procesy a procedury pro nakládání s atributy identit.

- **Správa identifikačních údajů**

Účinnost IDM systému závisí na procesech a správě identifikačních údajů. Tyto údaje slouží k identifikaci a autentizaci uživatele. Mezi identifikační údaje řadíme:

- Uživatelské jméno a heslo
- Digitální certifikáty
- Biometrické údaje
- Informace spojené s PKI (certifikát, kryptografické informace apod.)
- Chytré karty
- Identifikační tokeny

- **Protokolování a audit**

Audit je důležitou součástí systému pro řízení identit, provádí se zápisem logů do protokolu, systém pro protokolování a audit by měl obsahovat:

- Vytváření záznamu a provádění auditu při definovaných událostech pro provádění forenzní analýzy.
- Mechanizmy a postupy, které umožňují zpětné dohledání.

- Detekce nedodržení platných pravidel.
- Zajištěni dodržování právních předpisů, zákonů a norem.

- **Kontrolní funkce**

V distribuovaných systémech je nutné zajistit správný tok a synchronizaci informací patřící identitě na daná místa v systému.

- **Komunikace**

Mezi jednotlivými prvky systému je nutné zajistit komunikaci, při které dochází k výměně informacích o identitách v rámci vnitřní sítě, vnější sítě a federace.

- **Dodržování politik**

Zaručení anonymity, zaručení soukromí, vytváření a shromažďování o identitách, použití a šíření informací o identitách.

- **Zákon o ochraně osobních údajů**

Je to určitý soubor práv a povinností, které se vztahují na zpracování informací, údajů a dat o fyzických osobách. V ČR je ochrana osobních údajů regulována zákonem č. 101/2001 Sb., o ochraně osobních údajů.

4.1.2 Správa digitálních identit

Administrátorské a uživatelské funkce pro úpravu a vytváření identit, skupin a jejich informací.

- **Správa adresářů -** Automatické vytvoření potřebných účtů a zdrojů pro identitu na základě kritérií.
- **Automatická propagace -** Propagace identit a změn do všech propojených systémů.
- **Automatická sekvence -** Nastavení a automatické spouštění definovaných sekvencí na základě definované akce. Např. zaregistrování nového zaměstnance vytvoří i jeho email na základě definované šablony.
- **Delegovaná administrace -** Přesunutí pravomoci na jinou entitu.
- **Správce hesel -** Synchronizuje hesla a nabízí obnovu hesla automatikou.
- **Správa rolí v systému -** Poskytuje abstraktivní zapouzdření nad skupinu oprávnění a privilegií, které mohou majitelé mít přiděleny.
- **Federace -** Integrace více IdMS systémů. Uživatel může jednou identitou přistupovat k více systémům v doméně.

4.1.3 Řízení rizik

Procesy:

1. **Ohodnocení rizik**
    - **Analýza rizik** slouží k určení a identifikaci rizik
    - **Vyhodnocení rizik** slouží k určení jejich významnosti
    - Nástroj pro vedení procesu – **CRAMM**
    - Standard – ISO/IEC TR13335-3
    - Opatření ISO/IEC 27002
2. **Zvládání rizik** slouží pro výběr a implementaci opatření
3. **Akceptace rizik** slouží k rozhodování o přijatelnosti možných rizik
4. **Informování o rizicích**

Audit

Do centrálního úložiště se trvale ukládají data, která jsou využívána pro analýzu. Akce, která vyvolá audit, se nazývá auditovaná událost. [25]

Pro audit se využívají informace, jako jsou role uživatelů, uživatelské oprávnění, časy přihlášení, evidence výsledků minulých auditů, automatické logy generované systémem IdM atd.

Adresářová služba

Adresářová služba je aplikace poskytující informace o pojmenovaných objektech v adresáři. Je nezbytnou komponentou IdM. K těmto objektům je přistupováno většinou intenzivně pro čtení a není zde nutnost častých změn. Ve srovnání s databázovými systémy neobsahuje kontrolu integrity. Všechny informace jsou uloženy v objektech ve formě atributů, které jsou standardizovány. Často jsou zde informace o uživatelích, jako jsou pracovní pozice, telefon, email, atd.

Meta-adresář [26]

Zajišťuje tok dat mezi adresářovými servery a databázemi, slouží k zajištění synchronizace

mezi propojenými systémy. Obsahuje agenty, kteří hlídají změny v systémech a centrálním uložišti.

Virtuální adresář

Virtuální adresář nebo jeho služba je softwarová vrstva přinášející jednotné komunikační rozhraní mezi aplikacemi a systémem řízení identit. Představuje abstraktní vrstvu, která je umístěna mezi různými aplikacemi a proměnlivým prostředím platforem a adresářových služeb. Sjednocující vrstva je potřebná např. v databázích, webových službách atd. Sjednocuje zdroje dat do jednoho virtuálního a je ideální pro konsolidaci dat uložených v distribuovaném prostřední.

4.1.4 OpenIDM

OpenIDM je open-source projekt napsaný v jazyce Java. Zdrojový kód je dostupný pod licencí CDDL. [27] Toto řešení umožňuje synchronizaci objektů mezi datovým uložištěm a cílovými systémy, dále zahrnuje základní uživatelský self-service, synchronizaci hesel uživatelských účtů, vytváření uživatelských účtů, auditní logy a definici workflow. Pro produkční prostředí jsou používány databáze MySQL, MS SQL Server a Oracle. Lze neoficiálně použít i další databáze připojené pomocí **JDBC**[11]. OpenIDM umožňuje specifikovat Business pravidla, která jsou uplatňována během provisioningu. Pro integraci se systémy jsou využívány OpenICF konektory. Prostřednictvím těchto konektorů je možné provést integraci s LDAP implementací. Pomocí textových konfiguračních souborů se definuje mapování objektů na databázové tabulky, nastavení parametrů jednotlivých konektorů nebo popis atributů zpracovávaných během provisioningu.

[11] **Java Database Connectivity** – část programovacího jazyka Javy. Definuje programovací rozhraní (**A**pplication **P**rogramming **I**nterface) pro přístup k relačním databázím.

4.1.5 MidPoint

Midpoint je OpenSource IdMS napsaný v programovacím jazyce JAVA a dostupný pod licencí Apache Licence V2. [28] Mezi funkce tohoto systému patří provisioning engine, synchronizace uživatelských identit, workflow, auditní logy, reporty a podpora modelu RBAC. Systém umožňuje specifikovat business pravidla pro uplatňování provisioningu. Dále je implementována podpora vytváření základních reportů. Midpoint poskytuje také GUI.

4.1.6 Ekonomický software Pohoda

Organizace používá ekonomický software Pohodu. Tento software používají tisíce živnostníků, podnikatelů a firem nejen pro zpracování účetnictví, skladového hospodářství, majetkové evidence, personalistiky a mezd, ale i pro správu obchodních kontaktů a každodenní získávání aktuálních ekonomických a obchodních informací o svých firmách.

4.1.7 Systémové požadavky

Systémové požadavky [29] na tento software představují doporučené parametry pracovních stanic jednotlivých uživatelů programů STORMWARE Office. Lze je použít jako minimální parametry serveru file-serverových (síťových) verzí/řad programů STORMWARE Office.

- **Systém** je možný na platformách, které jsou v dnešní době nejrozšířenější – MS Windows 10, Windows 8/8.1 CZ, Windows 7 SP1 CZ nebo Windows Vista SP2 CZ a pro serverovou variantu Microsoft Windows Server 2012
- **Procesor**: Intel Core 2 Duo 2 GHz a pro serverovou variantu Intel Quad Core Xeon 2,5 GHz.
- **Paměť**: 2 x 2048 MB a pro serverovou variantu minimálně 8 GB RAM,
- **Pevný disk**: 2 x SATAII, 7200 ot./min.
- **UPS**: Doporučené volitelné příslušenství, které může zabránit ztrátě dat při výpadku proudu.
- **Tiskárna**: Laserová tiskárna a pro rychlý tisk paragonů pokladní tiskárna.

Síťové verze POHODA s označením NET umožňují pracovat s daty umístěnými na serveru až ze 3 stanic (v případě síťové verze NET3), resp. až 5 stanic (v případě síťové verze NET5) propojených do sítě. Pro další počítač jsou určeny přídavné síťové licence CAL.

POHODA využívá file-server technologii postavenou na databázovém stroji MS Jet, podobně jako známý kancelářský produkt Microsoft Access. U systémů POHODA SQL a POHODA E1 je použita technologie klient-server a databázové prostředí Microsoft SQL Server. Díky tomu dochází k výraznému zvýšení výkonu a bezpečnosti celé aplikace. Uživatelům je také umožněno bezproblémově a souběžně zpracovávat velké množství dat, aniž by docházelo k jakémukoliv zpomalení systému.

Každá aplikace vyžaduje pro svůj provoz technickou infrastrukturu (server, klientské počítače, síťové prvky a operační systémy) s parametry odpovídajícími zejména zatížení aplikace v plném provozu. Při síťové práci se po síti přenášejí značné objemy dat a na celkový výkon systému POHODA tak má rozhodující vliv optimální dimenzování všech prvků infrastruktury a jejich vyvážené sestavení.

4.2 Požadavky na systém

Základní funkční požadavky:

- Autentizace v aplikace se provádí pomocí uživatelského jména a hesla.
- Uživatel může měnit hesla u svých účtů.
- Uživatel může žádat o přiřazení a odebrání rolí a oprávnění.
- Systém je kompatibilní s nejrozšířenějšími systémy (MS. Windows, Linux, Mac OS).
- Systém umožňuje vytvářet auditní logy (lze dohledat hodnoty atributů).
- Systém využívá centrální datové uložiště pro uchovávání datových objektů.
- Systém umožňuje import uživatelských identit z datového souboru.
- Systém umožňuje integraci se systémem.
- Systém využívá centrální datové úložiště pro uchovávání dat.

4.2.1 Uživatelské role

- **Administrátor** - Administrátor má všechna oprávnění v rámci aplikace.

Je to správce, který má veškerá práva. Může zakládat nové firmy, přejmenovávat je, odpojovat, mazat, obnovovat ze seznamu odpojených firem i ze zálohy. Má neomezený přístup k auditním logům a přístup ke schvalovacím workflow.

- **Super uživatel (manažer)** - Super uživatel má téměř všechna oprávnění v rámci aplikace s výjimkou správy uživatelských účtů. Nemůže přidávat nové uživatele a měnit jejich přístupová práva. Může přidávat účetní období a měnit nastavení stávající firmy, číselníky a veškeré ostatní uživatelské práce, vč. zálohování dat.
- **Standardní uživatel** - standardní uživatel má nižší oprávnění než super uživatel. Může s aplikací pracovat, ale nemůže měnit nastavení a zálohovat data. Může si změnit heslo, má přístup do osobních certifikátů.

4.3 RBAC model

Podle analýzy modelové organizace bylo provedeno zjednodušení RBAC modelu [30] tak, aby byl vhodný pro malé a střední firmy.

Objekty RBAC:

- **Uživatelská identita**
- **Role**
- **Oprávnění**
- **Skupina**
- **Účet**

Subjekt je aktivní prvek modelu (u některých modelů člověk, jinde proces). **Objekt** je pasivní prvek (soubor, prvek, adresář apod.) **Proces** může být subjekt i objekt, záleží na tom, zda je v aktivní nebo pasivní roli.

Důvody k zavedení byly:

- Komplikovaná správa rozsáhlých systémů.
- Nemožnost efektivní distribuce práv k systému mezi více administrátorů.
- Požadovány dynamické změny práv.
- Problém s přidělování práv uživatelům – komplikovanost správy.

Přínos RBAC modelu

- Nemusí se používat nízko úrovňové přiřazování práv jednotlivcům.
- Identita uživatele může být nahrazena rolí (utajená) – vhodné ve webových aplikacích.
- Možnost hromadně měnit práva uživatelům v dané roli.
- Snížení možnosti vzniku chyby.
- Role korespondují s pozicemi, které uživatelé zastávají v organizaci a jsou popisnější.
- **Zavedení RBAC snižuje náklady a čas na správu systému**

2 základní přiřazeni

- **Uživatel – role**
- **Práva – role**

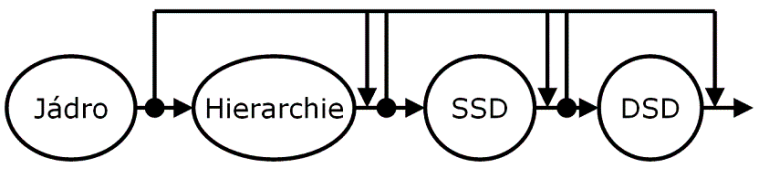
Role – odvozena od pracovní funkce v organizaci, má přiřazenou informaci týkající se autority a odpovědnosti z této funkce.

Roli jsou přiřazena práva:

- Přístupová práva k souboru
- Systémová práva

RBAC model je 4 stupňový:

- **RBAC0** – role nemají žádnou hierarchii, definovány pouze komponenty jádra RBAC
- **RBAC1** – zavádí hierarchii rolí
- **RBAC2** – zavádí statická omezení (SSD)
- **RBAC3** – zavádí dynamická omezení (DSD)



Obr. 5 Model RBAC

Přiklad práce v SELinux s RBAC rolemi [30]:

V SELinuxu je třeba RBAC explicitně spustit:

seedit-rbac on

reboot

Defaultně jsou to tyto 3 role:

• sysadm_r

• staff_r

• user_r

Změna role:

newrole -r sysadm_r

Authenticating root

Password:

Nastavení uživatele, role, práv (zápis do složených závorek):

role webmaster_r;

user webmaster;

allow /var/www/** r,w,s;

4.4 Použité technologie

4.4.1 JavaServer Pages

JSP je prezentační technologie umožňující jednoduchým způsobem vytvářet webové stránky. Obsah webových stránek je vytvářen pomocí tagů. Mezi základní tagy patří tagy jazyka HTML.

4.4.2 Twitter Bootstrap

Open-source Framework určený pro grafické uživatelské rozhraní **(GUI)**. Je kompatibilní se všemi oblíbenými prohlížeči.

4.4.3 Front Awesome

Poskytuje vektorové ikony a je vhodným doplňkem Twitter Bootstrap.

4.4.4 PostgreSQL

Bezpečný a rychlý Open-source databázový systém objektově relační.

4.4.5 Apache Maven

Softwarový nástroj pro správu a řízení procesu sestavování aplikací v Javě.

Stahování a importování důležitých knihoven do projektu.

4.4.6 Zdrojové systémy

Umožnují snadný import uživatelských identit. Komunikace probíhá pomocí REST webových služeb.

II. PRAKTICKÁ ČÁST

5 IMPLEMENTACE

Pro potřeby implementace byla provedena analýza řešení a vytvořena sada dokumentů pro plánování a vytvoření softwarového systému.

Jsou definovány potřeby pro zavedení správy identit a oprávnění. S implementací systému IdM je implementován jednotný nástroj pro správu identit, oprávnění a pro autentizaci. Nejdůležitějšími funkcionalitami IdM jsou automatické procesy synchronizace, které se starají o distribuci aktuálních dat a uživatelů z autoritativního systému do připojených systémů.

Uživatelské rozhraní IdM je zobrazitelné v prohlížeči uživatelů podle specifikace integračních platforem. Při zavedení systému pro řízení identit do prostředí bude konfigurace probíhat v prostředí dodavatele a následně bude systém převeden do integračního prostředí, kde se otestuje a doladí s využitím testovacích dat. Začlenění IdM do infrastruktury má za následek úpravu některých současných mechanismů a nastavení některých systémů, které jsou v rámci infrastruktury a jsou provozovány jinými dodavateli.

Definované konvence pro vytvářený software:

- Dodržování maximálního počtu znaků na řádku (obvyklá hranice je 100 znaků).
- Dodržování správného odsazení u kódu.
- Vytváření komentáře u metod a tříd.
- Vytváření inline komentáře u složitých implementací.
- Vytváření identifikátorů metod a proměnných.
- Psaní veškerého obsahu v anglickém jazyce.

Dalším prvkem aplikovaným při vývoji je tzv. programování proti rozhraní [31] tzn., že pro systémové komponenty existuje rozhraní a minimálně jedna implementace tohoto rozhraní. Tento přístup znamená flexibilitu a výměnu implementace.

5.1 Vývojové prostředí

NetBean od Oracle Corporation a **Eclipse** od Eclipse Fundation.

5.2 Správa kódu

Poskytování webového repositáře je webová služba Bitbucket.

5.3 Adresářová struktura aplikace

Struktura je rozdělena do dvou hlavních částí. První část je webový obsah, který je umístěn v adresáři */src/main/webapp*.

Druhou částí jsou třídy jazyka Java umístěné v adresáři */src/main/java*.

5.4 Front-end

Patří sem konkrétní implementace prezenční vrstvy a grafického rozhraní.

Prezenční vrstva je tvořena pomocí architektonického vzoru model-view-controller s využitím modulu Spring Web MVC.

Grafické rozhraní je implementováno s využitím front-endového frameworku Twitter Bootstrap. Prostřednictvím GUI je možné provádět kompletní správu uživatelských identit a objektů RBAC modelu. Také je možné vytvářet žádosti a spravovat jejich kompletní workflow.

5.5 Back-end

Popis konkrétní implementace servisní a datové vrstvy.

Servisní vrstva zapouzdřuje veškerou business logiku aplikace. Pro přenos dat doménových objektů mezi prezentační a servisní vrstvou jsou využívány tzv. update objekty.

V datové vrstvě jsou specifikovány doménové objekty, které jsou používány pro uchování dat. Doménové objekty jsou převedeny na databázové tabulky, kde atributy objektů tvoří sloupce databázových tabulek a na základě vztahu mezi objekty jsou vytvářeny klíče v tabulkách.

Doménové objekty jsou umístěny v balíku *cz.maxa.midm.core.model*. U každého objektu jsou používány JPA anotace pro specifikování způsobu mapování na databázovou tabulku.

Fyzický model dat je tvořen z definovaných doménových objektů pomocí Hibernate frameworku.

5.6 REST webová služba

Implementované webové služby slouží pro import uživatelských identit do systému. Existují dvě služby. První služba slouží k vrácení uživatelské identity na základě osobního čísla. Druhá k vytvoření nové uživatelské identity.

V implementaci systému firmy je navržen optimální způsob a vhodná forma řízení přístupu k informačním systémům. Byla zde provedena analýza a navrhnuto řešení. Firma má dvě divize, kdy každá z nich má několik poboček po celé zemi. Divize fungují jako samostatná organizace s vlastní organizační strukturou a různými aplikačními systémy.

5.7 Firemní strategické plánování

Strategické plánování minimalizuje dopad špatných řešení, která sice plní svou funkci i přinášejí výhody, ale nebývají přínosem pro celou organizaci. Proto se stalo zvykem vytvořit strategický plán pro správu identit, který bere pohled na funkcionalitu v dlouhodobém měřítku, a z toho plynoucí výhody i omezení celé společnosti. Má naplánovat pilířové části systému, které budou přinášet užitek napříč celou organizací.

5.8 Analýza firmy

Pro potřeby společnosti byla provedena analýza a vytvořeno několik dokumentů. Každý dokument je určen pro jinou fázi implementace. Od fáze implementace, plánování, analýzu možných řešení až po konečné nasazení. V různých fázích je potřeba různorodá míra podrobností o technických nebo manažerských detailech. Analýza se snaží definovat potřeby, které je nutné vyřešit při zavádění správy identit a oprávnění. Během implementace systému IdM je implementována jednotná správa identit, oprávnění a agendové aplikace. Díky IdM jsou data zaměstnanců načítaná z odpovídajících zdrojů např. z HR systému. Údaje o externích zaměstnancích jsou do systému zadávány přímo v IdM osobou k tomu

oprávněnou.

Ze systému jsou pak tyto informace předávány do odpovídajících systémů. Tím je proces správy uživatelů centralizován a zautomatizován. IdM pokrývá všechny procesy, které souvisí s identitou a rolemi tj. vznik identity, přiřazení oprávnění, odebrání a změna oprávnění a atributů, změna hesla, zrušení identity. Jedna z nejdůležitějších funkcí systému IdM jsou automatické synchronizace, které mají na starosti distribuci uživatelů a dat z hlavních databází do připojených systémů a proces rekonciliace rolí a uživatelů, které sledují stav uživatelů, uživatelských oprávnění a kontrolují, zda nedošlo k bezpečnostní chybě, např. existující neoprávněné účty atd. Nejdůležitější uživatelská funkcionalita je možnost zažádat o další role z webového rozhraní a administrace externích uživatelů.

V IdM existuje pro každou fyzickou osobu jedna globální identita a několik účtů na připojených systémech typu Active Directory, HR systém, Exchange, Sharpoint atd.

Uživatelské rozhraní je zobrazitelné v prohlížeči uživatele dle zvolené platformy. Obsahuje Branding společnosti a pro přístup používá SSO – přihlášení čipovou kartou a je přístupné všem interním i externím zaměstnancům. Uživatelům se speciálním oprávněním administrátor je přístupné administrátorské rozhraní. Pro potřeby kontroly a auditu je možné zobrazit reporty, které obsahují informace ze všech systémů.

5.9 Standard pro IdM[12]

Cílem dokumentu je definovat strategii směřující ke sjednocení řízení identit v rámci celé organizace.

Definuje požadavky na správu identit a oprávnění, globální identitu, bezpečnostní aspekty, principy schvalování v rámci systému řízení identit, standardizované přístupy k procesům správy uživatelských účtů, oprávnění a rolí.

[12] Part 6: Identity Management (IdM) Landscape: IdM standards, organizations and gap analysis. [32]

Tento dokument ovlivňuje identity – zaměstnance a externí identity.

Pokud se napojí další systémy, které odpovídají tomuto standardu, musí dojít k přesné technické realizaci. Tento dokument se musí aktualizovat minimálně jednou za rok.

Základními podmínkami pro dokument standardu IdM je sjednocení práce s identitami, sjednocení autentizační a autorizačních mechanismů a stanovení pravidel i politik, sjednocení technického rozhraní, sjednocení atributů identit napříč aplikacemi a napříč společností.

Předpoklady tvoří jednotná technologická platforma pro aplikace a systémy, jednotné skladiště identit, jednotné oprávnění, certifikační autorita pro vydávání certifikátů pro čipovou kartu a napojené systémy umožnují využití služeb jednotného skladiště identit.

5.10 Součásti standardu IdM

Nedílnou součástí dokumentu je definování, pro koho je určen, kdo ho schvaluje, aktualizuje, z čeho čerpá a jak bude v budoucnu navazovat na další implementace.

5.11 Cílový koncept a detailní technická specifikace

Cílový koncept je jeden z výstupů v projektu IdMS, který vychází ze standardu pro IdM a přidává detailnější pohled na implementaci se zaměřením na technickou stránku. Navazuje na něj dokument **DTS (D**etailní **T**echnická **S**pecifikace), který se zaměřuje na určení autoritativního zdroje pro každý atribut, specifikace vlastností podle typu identity (např. interní zaměstnanec), obsahuje databázovou strukturu IdMS, jednorázové migrační postupy a detaily o zálohování a obnově IdMS.

Možné přínosy

Přínosem jednotné správy identit je nesporné zvýšení bezpečnosti informačních systému. Umožňují úsporu času administrátorů, snížení možnosti přenosu chyb při zavádění nových systémů a snížení celkových bezpečnostních rizik.

Globální identita je zobecněnou identitou uživatelů informačních systémů ve společnosti.

Globální identita agreguje všechny atributy identity, které jsou uloženy v různých IS, kde sada základních atributů vychází z informací zjištěných při analýze prostředí společnosti.

Identita představuje logické pouzdro nad účty uživatelů v IS a aplikacích. Při řízení identit je nutné vymezit identity, které jsou spravované.

Spravované identity

- Vedoucí pracovník – identita zaměstnanec
- Identity existují v hierarchii uživatelů spravované systémem IdM
- Existuje identita, která je v pozici vedoucího pracovníka ke každé jiné identitě
- Identity jsou spravované IdMS

Zaměstnanec je identita, která má hodnotu dlouhodobé působnosti v systému. Některá oprávnění jsou nastavena automaticky dle pracovního zařazení a pro přístup do systému je vyžadováno ověření pomocí čipové karty (nebo tokenu) s certifikátem.

Nespravované identity

Mezi rysy těchto identit patří výlučná existence mimo IdMS. Jejich životní cyklus je zajištěn mimo systém IdM a je zajišťován jinými prostředky.

Patří sem:

- **Ad hoc účet** – má omezenou životnost a je vytvořen místním administrátorem z různých důvodů
- **Servisní účet** – má v podstatě neomezenou životnost a je jednoúčelový

Přihlašovací jméno

Na přihlašovací uživatelské jméno jsou kladeny požadavky:

- Délka maximálně 25 znaků
- Shoda s emailovou adresou z domény (např. @corporace.cz)
- Unikátnost

5.12 Životní cyklus identity

HR systémy řídí životní cyklus identity, přiděluje atributy a používají tzv. scénáře užití.

Scénáře:

- **Vytvořit identitu –** umožňuje vytvořit identitu, záznamy z HR systému jsou přenášeny do IdMs automatiky, pro každou identitu, která má autoritativní zdroj jsou záznamy vytvářeny automaticky. Pro identity s autoritativním zdrojem IdMs, je vytvořeno uživatelské rozraní pro obsluhu a týká se to především externích subjektů.

- **Zneplatnit identitu** – umožňuje zneplatnit identitu. Záznam není odstraněn z IdMs ani z připojených systémů je pouze označen za neplatný (např. kázeňský prohřešek). Ke zneplatnění v připojených systémem dojde až při IdM synchronizaci.

- **Zrušit identitu –** umožňuje zrušit identitu, tzn., že je nejdříve označen za zneplatněný a přesunut do určené organizační jednotky v AD a jsou mu současně odebrány veškeré role. V AD je zachována elektronická stopa, nedojde k fyzickému odstranění účtu.

- **Změnit / prohlížet atributy identity** – umožňuje prohlížet nebo měnit atributy. Atributy, které lze měnit jsou specifikovány cílovým konceptem. Oprávnění jsou odvozena od typu identit a vazeb k aktuálně přihlášenému uživateli a editace je vázaná na autoritativní IdMs

- **Prohlédnout přiřazené role –** umožňuje prohlédnout role navázané na zvolenou identitu. Prohlížení je omezeno na oprávnění přihlášeného uživatele.

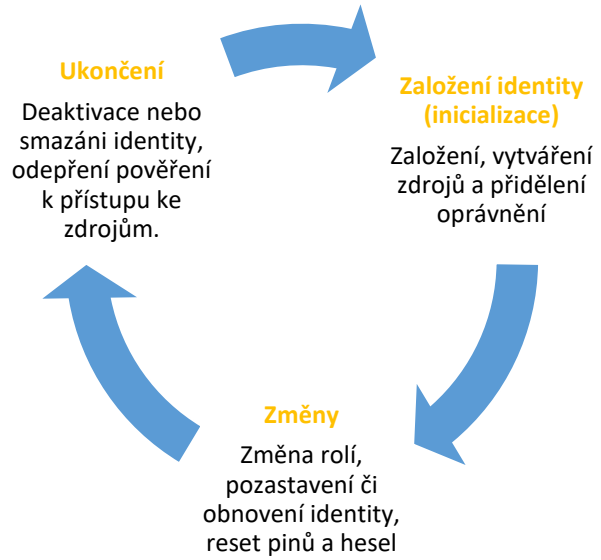
- **Přidělit / odebrat roli** – umožňuje přidělit a odebrat role zaměstnance. Role, které jsou určeny pracovní pozicí zaměstnance, jsou plně zautomatizované a nelze je odebrat. Všechny role musí být uloženy v registru rolí, například pomocí administrátora IdMs.

- **Schválit přiřazení a delegaci role** – umožnuje schválit nebo potvrdit přiřazené role a delegovat role pro které je aktuální uživatel garantem. Informace o garanci jsou uložené v databázi IdMs.

- **Delegace role** – umožňuje delegovat oprávnění mezi uživateli. Delegace je automaticky schválena, pokud je uživatel nadřízený a deleguje svou roli na podřízeného. Pokud uživatel deleguje role na svého spolupracovníka, je vyžadováno manuální schválení nadřízeným.

- **Provádět základní operace s daty v IdMs (CRUD) –** umožňuje provádět datové operace se záznamy IdMs. Především operace typu zobrazit, vytvořit, smazat a upravit, provádí pouze administrátor nebo poučená osoba**.** Špatný zásah může vést k nestabilitě nebo pádu systému. Používá se např. při napojování nové části systému.

5.12.1 Založení identity



Obr. 6 Životní cyklus identity

Identita Zaměstnanec je vytvořena ze záznamu z HR systému.

- Personalista založí záznam do HR systému.
- IdMs během synchronizace načte záznam z HR systému.

- Na základě pozice je založen účet a nastavena oprávnění v připojených systémech.
- Je zaslán email o založení účtu novému zaměstnanci a jeho nadřízenému.

Identita Externí subjekt (dodavatel, stážista atd.) je vytvořen na základě uživatelské žádosti a vyplněním formuláře pro založení identity.

- Uživatel musí vyplnit formulář v IdM.
- Žádost musí schválit vedoucí pracovník externích identit.
- Na základě schválení založí systém globální identity.
- Je zaslán email o založení účtu novému zaměstnanci, žadateli a schvalovateli.

5.12.2 Identita – Přejmenováni a změna

Identita Zaměstnanec – mění se na základě změn v HR systému.

- Personalista provede změnu ve svém systému.
- IdMs během synchronizace načte záznam z HR systému.
- Během aktualizace podle změn provede následující:
  - Aktualizuje údaje v připojených systémech a nastaví oprávnění podle atributů.
  - Změní globální identitu.
  - Přejmenuje.
- Je zaslán email o změně účtu uživateli, který žádal změnu.

Identita Externí subjekt – změna probíhá na požádání po vyplnění formuláře o založení nové identity.

- Uživatel v IdMs vyplní formulář.
- Žádost musí schválit vedoucí externích identit.
- Během aktualizace změn provede systém změny dle požadavků:
  - Změna údajů v globální identitě.
  - Aktualizuje údaje v napojených systémech a nastaví oprávnění v závislosti na atributech.
  - Případně přejmenuje.
- Zaslán email o změně účtu uživateli, který žádal změnu a schvalovateli.

Přejmenování

Pokud se přejmenovává účet, musí se manuálně zajistit návaznost používání účtu. Identitě,

která používá k přihlašování kartu s certifikátem, je nutné zajistit náhradní kartu s novým certifikátem na změněné jméno. To samé platí u identity, která se přihlašuje pomocí jména a hesla.

5.12.3 Identita - Zneplatnění

Zneplatnění identity provádí manuálně administrátor systému se stejným postupem pro všechny typy identit.

- Administrátor obdrží žádost o zneplatnění identity, tento požadavek vyhodnotí, a pokud je správný zadá ho do systému.
- IdMs provede zneplatnění účtu v napojených systémech a zneplatní globální identity.
- Zaslán email přímému nadřízenému.

5.12.4 Identita – Zánik

Zaměstnanecká identita zaniká změnou v HR systému (ukončení pracovní smlouvy).

- Personalista zadá záznam o ukončení pracovního poměru do HR systému.
- IdMs během synchronizace načte záznam a odebere oprávnění ve všech připojených systémech.
- Podle podnikové definice IdM zneplatní nebo zruší účty identit a poté zneplatní globální identitu.
- Zašle email s notifikací nadřízenému bývalého zaměstnance.

Externí subjekty

Identita externí subjekt zaniká na základě vyplnění formuláře o zrušení identity.

- Uživatel vyplní formulář v systému IdM..
- Formulář musí schválit vedoucí externích identit
- IdMs odebere oprávnění a podle podnikového definování zneplatní nebo zruší účty identity v napojených systémech a pak zruší globální identitu.

- Zaslán email vedoucímu externí identity.

5.12.5 Identita – Samoobslužné procesy

V systému řízení identit je pro běžného uživatele poskytováno samoobslužné rozhraní. Pomocí tohoto grafického rozhraní si uživatel může změnit heslo, zažádat o reset hesla nebo zažádat o novou roli.

Změna hesla

- **IdM**
  - Uživatel si může změnit heslo přes samoobslužné rozhraní v IdM a tento postup je stejný pro všechny identity.
  - Následně je heslo transferováno z IdM do napojených systémů, které používají IdM k řízení hesel.
- **Doména –** používá se u všech identit s přístupem do domény Windows
  - Uživatel použije dialogové heslo pro změnu hesla.
  - Změněné heslo je pomocí IdM předáno do napojených systémů, které používají heslo z IdM.

Reset hesla

- Uživatel pomoci GUI zažádá o reset hesla.
- Administrátor zkontaktuje uživatele (emailem, telefonicky atd.).
- Administrátor provede reset hesla a sdělí ho uživateli.
- Uživatel se přihlásí do domény a změní heslo.

Žádost o změnu oprávnění

- Uživatel se musí přihlásit do samoobslužného uživatelského rozhraní a vybrat akci „Žádost o změnu oprávnění“, potom vybere změnu oprávnění a identitu, které se změna týká.
- IdMs zaeviduje výsledek.
- Žadateli i schvalovatelům je zaslán email s výsledkem.

5.12.6 Identita – emailová upozornění (notifikace)

V IdMs je navrženo zasílání emailového upozornění (notifikace) o výsledcích operací.

Příjemci jsou **Uživatelé** (osoby, jejichž učet je měněn), **Žadatelé** (osoby, které operaci pro změnu identit inicializovaly) a **Schvalovatelé** (vedoucí osoby, oprávněné osoby). Pokud je schvalovatelů více, je zaslán email pouze tomu, který změnu inicializoval.

Upozornění obsahuje název systému a označení založeného účtu, výsledek postupů a nastavení atributu účtu.

5.13 Identity management – Microsoft Forefront Identity Management 2010[13]

Mezi klíčové vlastnosti produktu MS FIM 2010 patří samoobslužná správa identifikačních údajů, skupin a rolí firemních uživatelů, kompletní zautomatizování řízení životního cyklu identit. Program řídí, synchronizuje a zabezpečuje všechny data a poskytuje celou škálu nástrojů pro prosazování bezpečnostních politik firmy a audit.

Po celou dobu své životnosti je identita v relaci s integrovanými systémy.

Microsoft v tomto produktu slučuje několik technologií jako je operační systém **MS Windows** (FIM klient jsou koncové stanice a serverové verze operují s celou platformou), **MS Exchange server** (tato služba zahrnuje poštovní server, manažer kontaktů a kalendář), **MS AD** a **MS SharePoint** (tato služba sdílí zdroje a emailové zprávy). FIM je možné pomocí adaptéru spojit téměř se všemi systémy, které poskytují nebo získávají data, např. systémy lidských zdrojů, agendové systémy apod.

[13] FIM 2010 Technical Overview. [33]

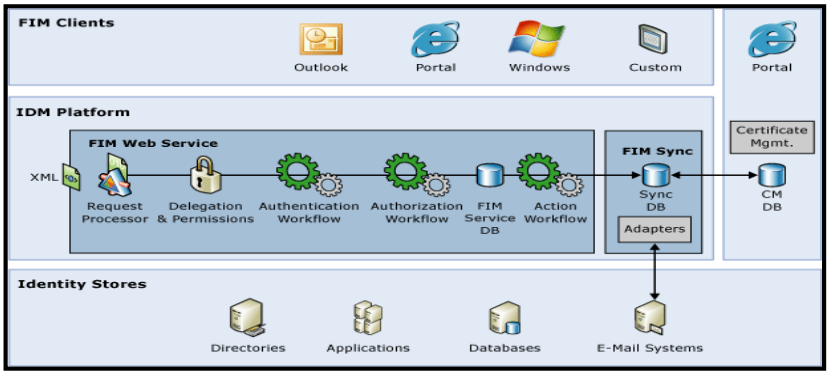
FIM patří do rodiny produktů **MS Forefront**, které jsou navrženy pro lepší ochranu sítí, koncových zařízení a serverů. MS Forefront je složen ze dvou částí – **FIM** a **UAG (U**nified **A**ccess **G**ateway). Tento produkt zajišťuje vzdálený přístup k firemním zdrojům zaměstnanci i externím identitám na stacionární i mobilní zařízení. Kombinuje různé možnosti připojení a má vestavené konfigurační politiky. Díky tomu poskytuje snadnou správu vzdáleného
přístupu z jakéhokoliv zařízení. FIM obsahuje **FIM Certificate Management**, který obsahuje databázi správ certifikátů. **Certificate Management Portal** jsou moduly certifikační autority, které jsou na CA serverech a klientech, u nichž je výměna dat vázaná na webové služby. FIM umožňuje přidat i certifikační autority od jiných firem.

5.13.1 FIM - architektura

FIM je složen z několika navzájem propojených komponent.

- **FIM klienti**
- **IDM platforma –** tato platforma je složena ze dvou částí
    - **FIM Web Service**, která zajišťuje prostředky pro zasílání požadavků k následnému zpracování pomocí definovaných workflow a může ovlivnit synchronizační službu.
    - **FIM Synchronization Service –** tato služba komunikuje s uložišti identit nebo je napojena k datovým zdrojům pomocí jejich adaptérů, které musí běžet na stejné stanici jako synchronizační služba a poskytuje přístup pomocí definovaného rozhraní k cílovým systémům (např. HR systém apod.).

- **Uložiště identity**



Obr. 7. Microsoft FIM 2010 diagram architektury[14]

FIM service

Obr. 8. FIM Service – postup zpracování požadavku

FIM service nabízí prostředky pro rozhraní WS (**W**eb **S**ervice). Tato komponente zodpovídá za zpracování všech požadavků FIM serverem a je nástrojem pro udělování politik. Požadavky jsou předávány přes rozhrání WS, kde jsou posléze vyhodnocovány, zda má uživatel všechna potřebná oprávnění k provedení požadavku. Nástroj pro řízení politik využívá **WF** (**W**indows **F**oundation) workflow. Jsou zde definovány pravidla, která se vykonají při určité činnosti nebo události.

Workflow

- **Autentizační workflow** – ověřuje pravost identity uživatelů. V případě nemožnosti ověření identity je požadavek odmítnut (např. obnova hesla pomocí samoobslužného rozhraní). Ověření může být pomocí certifikátu nebo sady údajů, které uživatel použil při registraci.

[14] FIM 2010 Technical Overview. [33]

- **Autorizační workflow** – umožňuje pokročilejší validaci oprávnění uživatelů. V případě nemožnosti ověření je požadavek zamítnut. Filtr může udělit rozhodnutí na základě obsahu požadavku a systémových pravidel. Např**.** změna osobních údajů - systém ověří, zda jsou zadaná data ve správném tvaru a odešle email na oddělení lidských zdrojů a nadřízenému.
- **Workflow akce –** poskytuje možnost systému vykonat akci poté, co byl požadavek řádně zpracován a proveden (např. změna atributu nebo změna hesla pomocí samo-obslužného rozhraní). Služba obnovení hesla pomocí workflow pošle požadavek synchronizační službě a okamžitě přenese změny do všech propojených systémů.
- **Databáze FIM Služeb** – FIM server využívá MS SQL server jako primární uložiště dat pro správu workflow, objektů, požadavků a politik. Po dokončení požadavku, než jsou změny promítnuty do celého systému pomocí synchronizační služby, jsou objekty, které jsou navázané na politiky, přesunuty na SQL server.

Synchronizační služba

Tato komponenta zodpovídá za synchronizaci dat mezi propojenými systémy, sdružuje informace o identitách do FIM metaverse systému a do všech datových zdrojů. Hraje také roli v bezpečnostní politice a slouží k výměně informací o identitách a jejich atributech při jejich založení.

FIM metaverse je datové uložiště, jehož hlavní funkcí je ukládání dat z propojených datových zdrojů v lokální kopii. Tato kopie se označuje jako datový prostor konektoru (connector space). Díky těmto nově uloženým datům může FIM synchronizační služba porovnávat nový a původní stav.

Zdroje identit jsou systémy, které FIM spravuje pomocí agentů řízení MA.

Zdroje identit obsahují tyto služby:

- Adresářové služby
- Certifikační služby
- Služby pro administraci čipových karet
- Databáze

- Síťové operační systémy
- Soubory
- SAP a další systémy

FIM klient je proces nebo entita, která komunikuje pomocí webové služby s FIM službou. Této službě dává příkazy pro vykonávání úprav, probíhá automaticky nebo poskytuje uživatelské prostředí, kde uživatel samostatně provádí potřebné úkony.

Klienti:

- Rozšíření pro MS Outlook, MS Windows, MS Exchange
- Windows Powershell
- Uživatelský portál FIM
- Synchronizační služba FIM

FIM – Synchornization Service Manager je administrativní rozhraní synchronizační služby vestavěné ve FIM Synchronization Service. Spravuje FIM Metarverse, synchronizační management agentů a jejich běhové workflow (run profiles). Používají jej pracovníci při instalaci systému a administrátor systému pro konfiguraci synchronizačního workflow a správu jednotlivých Management agentů v propojených systémech.

ZÁVĚR

Bakalářská práce „Správa identit a přístupů v informačních systémech“ je zaměřena na analýzu přístupů ke správě identit v IS a její aplikaci ve firmách. V teoretické části své práce jsem provedl rešerši správy identit a přístupů v IS. V praktické části jsem navrhl implementaci správy identit a vhodnou formu řízení přístupu v IS.

Cílem bakalářské práce byla analýza přístupu a správy identit pro malé podniky. Další částí tohoto cíle bylo ověřit hypotézu, zda IS v přístupu ke správě identit je přínosem pro firmy nebo znamená pouze náklady. Mohu konstatovat, že IS z tohoto pohledu je přínosem pro firmy a má dlouhodobý dopad. Práce ukazuje na oblasti, se kterými se setkáváme při analýze návrhu a implementaci řešení systému správy identit. Z těchto poznatků jsem navrhl řešení problému.

Vědecko-technický vývoj se promítá i do oborů jako jsou IS a IdM, kde bude znamenat další rozvoj a vytvoření standardů, které budou specifikovat nové přístupy v řízení identit a vztahů mezi nimi. Práce ukazuje na teoretický základ znalostí, podle nichž byl vypracován základní koncept řešení pro řízení identit ve firmách. Analýza byla provedena podle ekonomických možností a dané infrastruktury společnosti a na jejich základě bylo implementováno řešení v prostředí MS Forefront Identity Manager.

Identity Managemet je termínem zahrnující administraci individuálních identit (uživatelských účtů) v rámci určitého systému, např. firemních HR systémů. V podnikovém IT se správa identit týká jednotlivých rolí i práv pro jednotlivé uživatelské firemní sítě. Systémy identity dávají managementu a správcům IT nástroje a technologie potřebné ke kontrole přístupu uživatelů k podnikovým datům. Seznam technologií kategorie identity managementu zahrnuje nástroje pro správu hesel, softwaru, pro provisioning a deprovisioning, aplikace pro zajištění bezpečnostních pravidel, reportovací a monitorovací software a uložiště identit.

Proč je třeba se zajímat o identity management?

Správa identit souvisí s bezpečností a s produktivitou firmy působící v oblasti elektronických obchodních styků. Jsou využívány k ochraně digitálního majetku a ke zvýšení obchodní produktivity. Implementace systému pro identity management poskytuje mnoho výhod, např. zefektivnění chodu podniku. Úspěšná implementace vyžaduje předvídavost, je třeba míti vytyčené cíle a definované obchodní procesy. Hlavním rizikem jsou centralizované operace, které mohou být napadeny hackery. Access management referuje k procesům a technologiím využívaných pro kontrolu a monitorování přístupu k síti. Mezi funkce správy přístupu patří autentizace, autorizace nebo audit.

Technická inovace v tomto oboru (vývoj bezdrátových technologií) reaguje na potřebu efektivního podnikání, kde mobilita, bezpečnost, konektivita, flexibilita, pohodlí a služby pro zákazníky jsou klíčovými prvky pro podnikání. V jednadvacátém století se bezdrátové technologie začaly používat k běžným přenosům mezi jednotlivými uživateli a tento trend je ještě umocněn používáním mobilních zařízení.

Kryptografie neznamená dostatečnou ochranu pro správu identit a přístupů v informačních systémech. V současné době ještě nebyla vyvinuta ochrana, která by nemohla být proražena.

Systém pro správu identit poskytuje nástroje k implementaci komplexního zabezpečení, kvalitního auditivního procesu i vlastních pravidel pro přístup. Tyto systémy dnes nabízejí funkce určené k zajištění fungování organizace v souladu s regulacemi.

Jak bude vypadat vývoj v oblasti správy identit a přístupů v IS v budoucnu?

Vývoj se bude ubírat k další digitalizaci, jednotné mobilní platformě a budou se stírat rozdíly mezi soukromou a pracovní identitou. Věřím, že další rozvoj identity managementu bude mít vliv na vyšší efektivitu práce, spokojenost uživatelů i profit pro obchodníky.

SEZNAM POUŽITÉ LITERATURY

[1] SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (5. díl): Architektura IAM řešení. *IT Systems* [online]. 2015 (6) [cit. 2018-02-02]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-architektura-iam-reseni.htm

[2] Active Directory: Concepts Part 1. *Microsoft TechNet* [online]. [cit. 2018-02-05]. Dostupné z: https://social.technet.microsoft.com/wiki/contents/articles/16968.active-directory-concepts-part-1.aspx

[3] HAYDAY, Graham. IT users in password hell. *ZDNet* [online]. December 11, 2002 [cit. 2018-02-11]. Dostupné z: https://www.zdnet.com/article/it-users-in-password-hell/

[4] WAGNER, Ray. *Identity and Access Management 2020* [online]. June 2014. [cit. 2018-01-05]. Ke stažení dostupné z: https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/JournalPDFs/feature0614.pdf

[5] *Ottova encyklopedie A-Ž*. Praha: Ottovo nakladatelství, 2004, 1015 s. ISBN 978-80-7360-014-3.

[6] List of LDAP software. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-02-11]. Dostupné z: https://en.wikipedia.org/wiki/List_of_LDAP_software

[7] Active Directory: Understanding Proxy Authentication in AD LDS. *Microsoft TechNet* [online]. [cit. 2018-02-05]. Dostupné z: https://technet.microsoft.com/en-us/library/2008.12.proxy.aspx

[8] Active Directory Architecture. *Microsoft* [online]. 9 December 2009 [cit. 2018-02-05]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/bb727030(v=technet.10)

[9] SPEALMAN, Jill., Kurt. HUDSON a Melissa. CRAFT. *MCSE, exam 70-294: planning, implementing, and maintaining a Microsoft Windows Server 2003 Active Directory infrastucture : self-paced training kit*. Redmond, Wash.: Microsoft Press, c2004. ISBN 07-356-1438-5.

[10] ČECH, Pavel, Vladimír BUREŠ a Melissa. CRAFT. *Podniková informatika: planning, implementing, and maintaining a Microsoft Windows Server 2003 Active Directory infrastucture : self-paced training kit*. Hradec Králové: Gaudeamus, 2009. ISBN 978-80-7041-479-8.

[11] GALBA, Alexander a Antonín PAVLÍČEK. *Moderní informatika*. Praha: Professional Publishing, 2012, 184 s. ISBN 978-80-7431-095-9.

[12] SOMMERVILLE, Ian, Vladimír BUREŠ a Melissa. CRAFT. *Softwarové inženýrství: planning, implementing, and maintaining a Microsoft Windows Server 2003 Active Directory infrastucture : self-paced training kit*. Brno: Computer Press, 2013. ISBN 978-802-5138-267.

[13] COBIT. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-02-07]. Dostupné z: https://en.wikipedia.org/wiki/COBIT?oldid=468274501

[14] ŠČUREK, Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. *DocPlayer.cz* [online]. červen 2008 [cit. 2018-02-15]. Dostupné z: http://docplayer.cz/4922755-Biometricke-metody-identifikace-osob-v-bezpecnostni-praxi-studijni-text.html

[15] Access control. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-02-08]. Dostupné z: https://en.wikipedia.org/wiki/Access_control

[16] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné z: http://hdl.handle.net/10563/25821

[17] ApacheDS v2.0 Basic User's Guide. *Apache Directory* [online]. [cit. 2018-03-10]. Dostupné z: http://directory.apache.org/apacheds/basic-user-guide.html

[18] Red Hat Directory Server 8.1: Deployment Guide. *Red Hat* [online]. [cit. 2018-03-02]. Dostupné z: https://access.redhat.com/documentation/en-US/Red_Hat_Directory_Server/8.1/html/Deployment_Guide/index.html

[19] EDirectory 8.8 SP8. *Micro Focus* [online]. [cit. 2018-03-02]. Dostupné z: http://www.novell.com/documentation/edir88/index.html

[20] OpenLDAP. *OpenLDAP* [online]. [cit. 2018-03-02]. Dostupné z: http://www.openldap.org/doc/admin24/intro.html

[21] IBM Tivoli Directory Server, Version 6.3. *IBM Knowledge Center* [online]. [cit. 2018-03-04]. Dostupné z: http://www.ibm.com/support/knowledgecenter/SSVJJU_6.3.0/com.ibm.IBMDS.doc/welcome.htm

[22] Redmine. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-03-08]. Dostupné z: https://cs.wikipedia.org/wiki/Redmine

[23] Ganttův diagram. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-03-08]. Dostupné z: https://cs.wikipedia.org/wiki/Ganttův_diagram

[24] Deset kroků ke snadnější správě přístupu. *Security World* [online]. 2010, 2010(4) [cit. 2018-03-08]. ISSN 1802-4505. Ke stažení dostupné z: https://www.ami.cz/download/PR_clanky/Security_World-komlet.pdf

[25] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013 [cit. 2018-03-08]. ISBN 978-80-7251-397-0.

[26] LOOMES, John. Microsoft Metadirectory Services - an overview. *ServerWatch* [online]. 7 Feb 2001 [cit. 2018-03-10]. Dostupné z: https://www.serverwatch.com/tutorials/article.php/1549011/Microsoft-Metadirectory-Services--an-overview.htm

[27] Common Development and Distribution License 1.0. *Open Source Initiative* [online]. [cit. 2018-03-11]. Dostupné z: https://opensource.org/licenses/CDDL-1.0

[28] Apace License. *The Apache Software Foundation* [online]. January 2004 [cit. 2018-03-10]. Dostupné z: https://www.apache.org/licenses/LICENSE-2.0

[29] Systémové požadavky pro produkty STORMWARE Office. *Stormware* [online]. [cit. 2018-03-12]. Dostupné z: https://www.stormware.cz/systemove-pozadavky/

[30] ZUKAL, Martin. *RBAC* [online]. [cit. 2018-03-14]. Ke stažení dostupné z: https://www.download.zcu.cz/public/Prezentace/seminare%20CIV%202010/bezpecnost_linux/zukal-rbac.pdf

[31] Interface (programová konstrukce). In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-03]. Dostupné z: https://cs.wikipedia.org/wiki/Interface_(programov%C3%A1_konstrukce)#Programov.C3.A1n.C3.AD_proti_rozhran.C3.AD

[32] Part 6: Identity Management (IdM) Landscape: IdM standards, organizations and gap analysis. *ITU* [online]. [cit. 2018-04-02]. Dostupné z: https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part06.aspx

[33] FIM 2010 Technical Overview. *Microsoft* [online]. 14 November 2011 [cit. 2018-04-08]. Dostupné z: https://technet.microsoft.com/en-us/library/ff621362(v=ws.10).aspx

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACI	Access Control Instruction
AD	Active Directory - adresářové služby LDAP
AES	Advance Encryption Standard – mezinárodní šifrovací standard
AM	Access Management – správa přístupů
BER	Basic Encoding Rules – základní kódovací pravidla
COBIT	Control Objectives for Information and related Technology – mezinárodní standard pro správu a řízení informatiky
CRAMM	Central Risk Analysis and Management Method – analýza rizik správy identit
DES	Data Encryption Standard – standard pro šifrování dat
DIT	Directory Information Tree – stromová struktura informací
DoS	Denial of Service – odepření služby
DS	Domain system – systém domén
ERP	Enterprice Resource Planning – rovina celopodnikových systémů
GPO	Group Policy – nástroj pro hromadnou správu oprávnění
GUI	Graphical User Interface – grafické uživatelské rozhraní
GUID	unikátní identifikátor objektu
IAM	Identity Access Management – správa identit uživatelů
ICT	Information and Communication Technologies – informační a komunikační technologie
ID	Digital Identity – obecný atribut
IDEA	Internetion Data Encryption Algoritm – symetrická bloková šifra
IdM	soubor nástrojů, který se zabývá správou entit
IS	informační systém
IT	informační technologie

ITIL	Information Technology Infrastructure Library – soubor postupů zaměřujících se na využívání informačních technologií
LDAP	Lightweight Directory Access Protokol
PC	Personal Computer – osobní počítač
RAID	Redundant Array of Independent Disks – vícenásobné diskové pole
RBAC	Role Based Access Control – přístup na základě rolí
SASL	Simple Authentication and Security Layer – framework zásuvných modulů
SID	Security Identifier – unikátní identifikátor uživatele
SOA	Service Oriented Architecture – architektura orientovaná na služby
SSO	Single Sign On – technologie jednotného přihlašování

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: CD

Obsahem přiloženého CD je bakalářská práce v elektronické podobě.