

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



Implementace IdM řešení ve společnosti ALD Automotive s.r.o.

BAKALÁŘSKÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Autor: Jonáš Jandák

Vedoucí bakalářské práce: Ing. Jiří Sedláček, Ph.D.

Praha, květen 2019

Prohlášení

Prohlašuji, že jsem bakalářskou práci Implementace IdM řešení ve společnosti ALD Automotive s.r.o. vypracoval samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 2. května 2019

.....

Jonáš Jandák

Poděkování

Rád bych poděkoval vedoucímu mé práce Ing. Jiřímu Sedláčkovi, Ph.D. za jeho pomoc a cenné rady při psaní této bakalářské práce. Dále bych rád poděkoval Tomáši Lupkovi a kolegům ze společnosti ALD Automotive s.r.o. za možnost realizace řešení a pomoc během celého projektu. Na závěr také děkuji své rodině a přátelům za podporu nejen při vypracování této práce.

Abstrakt

Práce se zabývá problematikou identity managementu. Popisuje principy, specifika, přínosy a dopady v obecné rovině i jeho praktické zavedení do prostředí reálné společnosti ALD Automotive s.r.o. Poskytuje pohled na problematiku řízení a správy elektronických identit ve společnosti. Teoretická část práce se formou rešerše dostupných informací a jejich syntézy zaměřuje na samotnou definici a představení problematiky identity managementu. Hlavní cíl práce představuje implementace a konfigurace vybraného nástroje Evolveum MidPoint do reálné společnosti ALD Automotive s.r.o. při splnění stanovených požadavků. K jeho dosažení vede cesta přes několik dílčích cílů, které zahrnují vymezení základních zákonitostí problematiky řízení a správy elektronických identit, analýzu možných řešení a výběr dodavatele, analýzu procesů a pravidel vztahujících se k dané problematice, až po samotné nasazení a konfiguraci nástroje Evolveum midPoint. Přičemž je kladen důraz na snadnou a intuitivní obsluhu identit pro běžné uživatele, protože identity management nepřináší vysoký prospěch pouze pracovníkům IT oddělení, ale i všem zaměstnancům od běžného pracovníka po nejvyšší vedení. Výstupem práce je základní vhled do problematiky řízení identit, přehled základních funkcí a vlastností identity managementu, porovnání výhod a nevýhod těchto řešení a postup implementace zvoleného řešení do produkčního prostředí společnosti ALD Automotive s.r.o. Práce tak může být použita jako podklad pro výběr a implementaci identity managementu do vlastní společnosti.

Klíčová slova

access management, bezpečnost, Evolveum midPoint, identita, identity management.

JEL klasifikace

M15, L86.

Abstract

This thesis is focused on the issue of the identity management. It describes principles, specifics, benefits and impacts in general and the practical implementation into the real company ALD Automotive s.r.o. Thesis provide insight into the issues of management and administration of digital identities in company. The theoretical part of the thesis, in form of a research of available information and its synthesis, is focused on the definition and presentation of the issue of the identity management. The aim of this work is describe the whole process of the practical implementation. To achieve it, some particular aims like define the basic principles of management and administration issues of digital identities, the analysis of possible solutions and selection of a supplier, the analysis of processes and rules related to the issue, and installation and configuration of the identity management solution Evolveum midPoint must be accomplished. Focused on an easy use and an intuitive work with the identities for standard users, the identity management is not only beneficial to IT staff but also to all employees, from a standard employee to the top management. The output of the thesis is a basic insight into the issue of the identity management, overview of the basic functions and characteristics of the identity management, comparison of advantages and disadvantages of these solutions and the process of implementation of the chosen solution into the production environment of ALD Automotive s.r.o. Thus, this thesis can be used as a basis for the selection and implementation of the identity management into one's company.

Keywords

access management, Evolveum midPoint, identity, identity management, security.

JEL Classification

M15, L86.

Obsah

Úvod.....	7
1 Identity management	9
1.1 Definice	9
1.2 Výhody, nevýhody a rizika	10
1.3 Cílové skupiny	11
2 Základní funkce a vlastnosti.....	13
2.1 Entita, identita	13
2.2 Životní cyklus identity	15
2.3 Workflow	15
2.4 Tvorba a správa identit	17
2.5 Autentizace a autorizace	18
2.6 Logování a audit	19
2.7 Integrace	20
2.8 Samoobsluha	21
3 Implementace IdM do prostředí reálné společnosti.....	22
3.1 Analýza současného stavu.....	22
3.2 Definice požadavků	24
3.3 Výběr řešení.....	25
3.3.1 Rešerše možných dodavatelů.....	25
3.3.2 Evolveum midPoint	26
3.3.3 GAPP System spol, s.r.o.....	28
3.4 Nasazení a konfigurace	28
3.4.1 Analýza skupin a identit.....	29
3.4.2 Definice rolí, meta rolí a oprávnění	29
3.4.3 Napojení Active Directory	32
3.4.4 Práce s uživatelskými účty.....	34
3.4.5 Uživatelská samoobsluha	35
3.4.6 Zhodnocení nasazeného řešení	35
3.5 Doporučení pro implementaci	36
Závěr	40
Použitá literatura.....	42

Úvod

Identity mangement, do češtiny překládaný jako řízení identit, spadá do oblasti počítačové bezpečnosti. Informační technologie a systémy dnes již považujeme za běžnou součást našeho života, a to i přesto, že pro ně je a ještě stále bude charakteristický velmi rychlý vývoj. Spolu s tím, tak vznikají požadavky nejenom na bezpečnost, ale také na efektivitu IT sektoru. V souvislosti s identity managementem můžeme mluvit o zefektivnění procesů, správy, zvýšení zabezpečení a v neposlední řadě o snížení nákladů. V současné době se lidé i společnosti v návaznosti na řadu úniků, odhalení a znepokojivých zpráv začínají více zajímat o svou digitální identitu a s ní spojenou bezpečnost.

Můžeme skoro s jistotou říct, že dnes si již každý uživatel internetu nebo zaměstnanec společnosti, alespoň jednou zažil vytváření nějakého účtu. Málokdy ale zůstane pouze u jednoho účtu a než se nový zaměstnanec stačí rozkoukat, je mu přidělen účet do počítače, e-mailové schránky, několika interních aplikací, výplatního systému, k tiskárnám a několika dalším aplikacím dodavatelů. V ideálním světě by člověk měl jeden účet (digitální identitu) na vše. Bohužel, ani digitální svět není ideální. Přesto se společnosti alespoň snaží o co největší centralizaci, a právě taková řešení nazýváme identity management. Tato problematika se samozřejmě dotýká také IT administrátorů, na nichž spočívá správa všech přístupů, obnovování hesel uživatelů, vytváření nových identit, jejich rušení a úpravy oprávnění. Ač se na první pohled jedná o rutinní a jednoduché úkony, tato operativní činnost může mnohdy zabrzdit nebo úplně zastavit rozvoj dalších oblastí infrastruktury a administrace.

S výše popsaným, jde ruku v ruce bezpečnost. Ve společnosti potřebujete vědět s absolutní jistotou, že přes konkrétní účet se přihlašuje opravdu jeho majitel, nebo potřebujete uživateli nastavit specifická oprávnění a v těchto případech není prostor pro chyby. S problematikou bezpečnosti se proto často pojí výraz access management neboli řízení přístupu.

Jak vidno, identity i access management se vhodně doplňují a v některých oblastech dokonce překrývají. Pokrývají ale širokou oblast problémů, a právě z tohoto důvodu jsou s danou problematikou spojovány oba výrazy identity a access management, ať už jako celek nebo samostatně, také se pro ně můžeme setkat s označeními IdM, IAM, IM apod. Platí zde, že mnoho autorů, mnoho názorů, a proto je vždy dobré věnovat na začátku chvíli času ujasnění v jakém kontextu a rozsahu se problematikou budeme zabývat, a to jak v teoretické rovině, tak i při praktickém použití.

Motivací pro sepsání této práce byla, mimo jiné aspekty, i situace ve společnosti, kde autor pracuje. Společnost se postupně rozrůstá, jak do počtu stálých zaměstnanců, externistů, dodavatelů, tak i počtem různých informačních systémů. Vedení IT oddělení tedy po analýze vytížení infrastrukturní části usoudilo, že zavedení identity managementu, by mělo přinést společnosti větší efekt, než jaké jsou náklady na jeho zavedení. K rozhodnutí také vedla časová náročnost úkonů, které je možné automatizovat, jako je zakládání nových účtů, jejich rušení, editace, změna oprávnění. Dalším důvodem bylo zvýšení bezpečnosti. Stává se, že nadřízený IT oddělení neinformuje o odchodu svého zaměst-

nance, a tak není problém v systémech narazit na tzv. černé duše, což samozřejmě představuje značný bezpečnostní problém a přináší to i zdánlivé maličkosti, jako je neefektivní nakládání s licencemi, které výsledně může společnost stát nezanedbatelné finanční prostředky.

Práce analyzuje a vymezuje základní zákonitosti problematiky řízení a správy elektronických identit ve společnosti. Teoretická část popisuje a vysvětluje základní vlastnosti a funkce identity managementu a seznamuje s nimi čtenáře. Jedná se o autorův pohled, který byl tvořen rešerší článků a knih pojednávacích o dané problematice a zkušenostmi kolegů. Za tímto účelem bylo použito převážně metody analýzy a syntézy shromážděných informací o dané problematice. Není zde tedy podán vyčerpávající popis všech možných metod a oblastí, protože v tomto odvětví, které se stále vyvíjí a rozšiřuje, by to byla zbytečná až nemožná snaha.

Hlavní cíl práce představuje implementace a konfigurace vybraného nástroje Evolveum MidPoint do reálné společnosti ALD Automotive s.r.o. při splnění stanovených požadavků. K jeho dosažení vede cesta přes několik dílčích cílů, které zahrnují vymezení základních zákonitostí problematiky řízení a správy elektronických identit, analýzu počátečního stavu prostředí a definici očekávání. Dále následuje analýza a rešerše dostupných řešení, jejich vyhodnocení a interní výběrové řízení na implementátora. V neposlední řadě je třeba vytvořit plán realizace, provést řadu interview s vedoucími pracovníky oddělení, zahájit samotnou implementaci a vypořádat se s jejími nástrahami, spolu s konfigurací přímo pro potřeby společnosti. Při zpracování této části práce bylo využito osobních zkušeností z celého procesu implementace. Zdrojem poznání bylo i pozorování a konzultace s odborníky v oblasti identity managementu.

Závěr práce obsahuje zhodnocení celého průběhu implementace pohledem autora a jím navržený doporučený postup při výběru a implementaci libovolného řešení identity managementu spolu s možnými překážkami, které mohou během nasazení nastat. Práce předpokládá alespoň základní čtenářovu znalost v oblasti bezpečnosti informačních technologií.

1 Identity management

S pojmem Identity management (IdM), nebo jinak také řízení identit, se setkáváme v oblasti bezpečnosti informačních systémů společnosti, a s tím spojenou správou uživatelských dat. V dnešní době má prakticky každá trochu větší společnost podnikový informační systém, který zastřešuje určité informační systémy, jejichž množství se s postupem času a rostoucí velikostí společnosti navyšuje. Ve společnostech běžně pracují mimo stálých zaměstnanců i externisté a dodavatelé dalších systémů. Pracují odkudkoliv a kdykoliv. To vše rapidně navyšuje požadavky na bezpečnost a efektivitu v oblasti správy elektronických identit.

Interaktivita a personalizace se dá považovat za jedny z hlavních charakteristik pro digitální svět, tak jak ho známe dnes a jak se bude pravděpodobně dále vyvíjet. Čím dál více se individualizuje a interaguje přímo s konkrétním uživatelem. Již nestačí informace či obsah masově rozšířit bez znalosti příjemce, a proto musí být dnešní digitální svět založen na identitách, jejichž osobní údaje jsou schraňovány, analyzovány a hojně využívány. To na druhé straně přináší ztrátu určité části bezpečnosti, která je spojena například s krádeží identity, zásahy do soukromí nebo zneužitím osobních údajů. Příkladem může být vyčíslení škod spojených s krádeží identit za rok 2017 pouze ve Spojených státech amerických v celkové výši 16,8 miliard amerických dolarů (Pascual et al. 2018).

Právě identity management zvyšuje zabezpečení a produktivitu práce, jak na straně uživatelů, tak i správců informačních systémů. Konzistenci a komplexnost bezpečnostní politiky podporuje centralizovaný přístup ke správě účtů a oprávnění. Identity management přináší také možnost dokumentovat činnost a poskytuje tak kvalitní podklady pro interní i externí audity. Vrcholnému managementu společnosti poskytuje informace pro optimalizaci a přizpůsobení společnosti potřebám zaměstnanců i jejich partnerů.

1.1 Definice

Někdy se v této oblasti používá výraz Identity and Access Management (IAM), jelikož řízení identit můžeme rozdělit na dva pohledy, a to správu identit, neboli identity management, a řízení přístupu, tedy access management, který se zabývá přístupy a oprávněními (autentizací a autorizací) v rámci různých systémů, které společnost používá, což vede k dodržování bezpečnostních zásad a nařízení společnosti. V této práci bude termín identity management využíván pro celek řízení identit.

Společnost Gartner definuje identity management takto (Gartner Inc. 2019; překlad autor): „*Identity a Access Management je bezpečnostní disciplína, která umožňuje oprávněným osobám přístup k určitým zdrojům ve vhodnou dobu a ze správných důvodů.*“

IAM řeší zásadní potřebu zajistit odpovídající přístup ke zdrojům v rámci stále více heterogenního technologického prostředí a splňovat stále přísnější požadavky na

dodržování předpisů. Tato bezpečnostní praxe je zásadní záležitostí pro jakoukoli společnost. Je stále více zaměřená na podnikání a vyžaduje obchodní znalosti, a nikoli jen technickou odbornost.

Společnosti, které vyvíjejí vyspělé IAM řešení mohou snížit náklady na správu identit, a co je ještě důležitější, stávají se značně agilnější v podpoře nových podnikatelských iniciativ.“

Český dodavatel BVC Solution definuje IdM následně (Cirkva 2018): „*Identity management (IdM) je centralizovaná správa identit v IT systémech. Umožňuje správným osobám přístup ke správným zdrojům, ve správný čas, ze správných důvodů a s plnou evidencí. IT systémy jsou typicky heterogenní a jsou dostupné po interní síti. Správa je prováděna zásahem administrátora v IdM nebo automatizovanými procesy.*“

Pokud vycházíme z těchto dvou definic, tak můžeme říci, že hlavní podstata řešení spočívá v automatizované, centralizované správě uživatelů, kteří jsou reprezentováni jedinečnou digitální identitou. Ta definuje jednu reálnou osobu a po založení v systému je udržována, spravována a monitorována během jejího celého životního cyklu, který je díky identity managementu efektivní a jasný. Administrátoři disponují nástroji pro správu rolí, jejich změnu, monitorování aktivit a k uplatňování bezpečnostních zásad.

1.2 Výhody, nevýhody a rizika

Nasazení IdM řešení přináší společnosti obecně mnoho výhod. Snaží se přispět k ochraně dat, která právem považuje za aktiva, zajistit efektivní správu a ve výsledku také ušetřit náklady spojené s bezpečností a IT provozem. Na výhody, které implementace přináší, se dle mého názoru, můžeme dívat ze tří pohledů.

Z technologického pohledu, centralizace a automatizace správy může přinést redukci nákladů, objemnosti a náročnosti systému jako celku. Dále zajišťuje konzistentní nastavení a dodržování bezpečnostních politik společnosti. Nabízí jednotné, centrální rozhraní pro komunikaci mezi informačními systémy společnosti. Konsoliduje procesy pro práci s identitami, z čehož plyne zjednodušení a zpřesnění celého návrhu a všech případných opatření.

Druhým pohledem může být bezpečnost společnosti. Zde IdM přináší jasně definované, dobře říditelné a bezpečné přístupy, což ocení jak správci systémů, tak i běžní uživatelé. O to více v době, kdy společnosti povolují přístup do svých interních systémů vlastním uživatelům, externistům, dodavatelům či zákazníkům a to i mimo organizaci. To vše vede ke zvýšení spokojenosti uživatelů a efektivitě při snížení nákladů. Nesmíme zde zapomenout na nástroje pro reporting aktivit, které IdM řešení také obsahují. Ty mohou sloužit vyššímu managementu, IT oddělení nebo auditorům.

Posledním pohledem je samotný uživatel. Ten jistě přivítá zjednodušený a minimálně částečně automatizovaný proces získání přístupu a následné autorizace do aplikací. Také možnost samoobsluhy, díky které může určitá svá data a oprávnění spravovat z jednoho místa sám. Zautomatizování workflow zjednoduší práci administrátorům například tím, že

celé vytvoření účtu provede samo na základě definovaných pravidel a postupů. V poslední řadě je vhodné zmínit automatické detekce a predikce možných chyb a problémů, které zvyšují zabezpečení, efektivitu a šetří čas.

Nevýhody můžeme spatřovat převážně v procesu implementace, který vyžaduje vynaložit určité úsilí od větší části společnosti, ne pouze IT oddělení. Dále sem můžeme zařadit vysoké počáteční náklady, pracnost a náročnost samotného zavedení IdM řešení, zvýšené nároky na uživatele a zodpovědnost vedoucích pracovníků.

Investiční náklady spojené s celým projektem a rizikovost instalace nelze dopředu plně vyjádřit, protože pro implementaci IdM platí, že je prakticky pokaždé unikátní, neexistují dvě stejná řešení. V průběhu implementace vzniká riziko ztráty nebo poškození dat při migraci a napojení IdM do práce s uživatelskými účty. Všechny systémy musí být buď vhodně zálohovány, nebo musí proces napojení IdM probíhat velmi obezřetně a podléhat důkladnému testování.

Rizikem IdM řešení z pohledu bezpečnosti je možná krádež dat. Vzhledem k centralizaci, v případě úspěšného útoku na databázi IdM systému, budou odhalena data do všech nebo většiny systémů. V případě, že útočník zjistí heslo uživatele, získá tím přístup do všech nebo většiny systémů uživatele, což je oproti principu, jeden systém = jedno heslo, značný rozdíl.

Za nevýhodu může uživatel považovat také fakt, že IdM systémy monitorují a zaznamenávají jeho aktivitu, a tak je pod větším dohledem.

1.3 Cílové skupiny

Cílovou skupinou je specifický okruh zákazníků, v našem případě společností, na které dodavatel cílí své produkty a služby, v našem případě identity management. Z pohledu marketingu je lepší nejdříve poznat svého zákazníka, a poté na něj vhodně cílit, namísto vystřelení nábojů naslepo s nadějí, že některý z nich trefí cíl. Kdo by tedy vůbec měl identity management používat? Pro koho je určen, co všechno ovlivňuje a komu co přinese?

Uvažovat o identity managementu by měla každá společnost, která nějakým způsobem využívá informační technologie a která čítá více než jednoho zaměstnance. Právě s informačními technologiemi přichází potřeba zajistit bezpečnost dat proti jejich zneužití nebo neoprávněné manipulaci. Možnost přístupu do systému vytváří bezpečnostní hrozby a právě uživatel je často slabý článek bezpečnosti. Míra rizika se navyšuje s přibývajícím počtem spravovaných uživatelů, rolí a otevřeností aplikací vně společnosti. Schopnost urdit všechny účty v dostatečném čase může být poté velmi náročné a je na každé společnosti, jestli se nechá zahltit agendou a například rezignuje na část svých bezpečnostních nároků, nebo bude hledat efektivnější cesty správy.

Nedá se jednoznačně identifikovat počet zaměstnanců, velikost společnosti, počet oddělení či jiný ukazatel, který by říkal, že společnost potřebuje identity management ve své plné síle. Je ale rozumné na řízení identit myslet již od počátku fungování společnosti. Na

začátku si pravděpodobně společnost vystačí s jednoduššími nástroji pro efektivní řízení identit. Růst společnosti se i v této oblasti samozřejmě pojí se zvyšujícími se náklady, nároky na efektivitu, audity a získávání přehledu o aktivitách uživatelů. Přírozně dochází ke změně vnitřních procesů společnosti a hledání možností zefektivnění a urychlení. V tuto chvíli přichází čas začít se zajímat o systémy pro správu a řízení identit, nebo v ideálním případě postupně rozvíjet stávající řešení v mocný nástroj, zvaný identity management.

Obecně vzato bezpečnost a rychlost spolu s určitou mírou uživatelského pohodlí nejdou úplně ruku v ruce. Je tedy nutné hledat hranici mezi uživatelským pohodlím a požadovanou úrovní zabezpečení. Proto vždy vzniká otázka, co je nutné po uživateli vyžadovat a zda některá restrikce není naopak kontraproduktivní. Například, jak moc je uživatelsky přívětivé, když se zaměstnanec musí přihlašovat do několika aplikací různými a složitými hesly, která musí co měsíc měnit? Studie Norského Centra pro Informační Bezpečnost z roku 2012 napříč norskou společností (NorSIS 2012) uvádí, že běžný zaměstnanec měl v průměru minimálně devět hesel vázaných pouze k pracovním povinnostem, přičemž pro ulehčení zapamatování hesla uživatelé použili běžná slovní spojení nebo si je prostě někde poznamenali. Studie společnosti Elcomsoft z roku 2009 (Elcomsoft 2009), která proběhla mezi IT specialisty převážně z Evropy a Severní Ameriky dokonce uvádí použití více než deseti hesel u 50 % dotázaných. Identity management se snaží těmto situacím předcházet pomocí jednotného přihlášení a uživatelsky přívětivé možnosti si zapomenuté heslo sám změnit bez nutnosti často zdlouhavé kooperace s IT podporou.

Níže je nastíněno, jak přínosy identity managementu můžeme sledovat napříč celou společností:

- Audit – snížení rizik a nastavení validních bezpečnostních kontrol.
- Finance – snížení nákladů.
- IT – efektivita a centralizace, management, snazší a rychlejší administrace, snížení požadavků a incidentů od zaměstnanců.
- Strategie – platforma pro budoucí růst a centralizaci služeb.
- Zaměstnanci – produktivita.

Důvodů pro zavedení identity managementu je napříč celou společností mnoho a každá společnost si je musí vyhodnotit individuálně. Měla by si ale uvědomit jaké má požadavky na bezpečnost, uživatelskou přívětivost, jaké technologie používá a jaké náklady, v souvislosti se zmíněným, vynakládá. Identity management můžeme spojit s bezpečností a produktivitou společnosti, která se snaží najít rovnováhu mezi požadavky na bezpečnost a mezi rychlostí přístupu a komfortem uživatelů.

2 Základní funkce a vlastnosti

Tato kapitola nastiňuje a snaží se vysvětlit dle autora základní funkce a vlastnosti systémů identity managementu. V každé její části popisuje i obecně používané termíny z této oblasti.

2.1 Entita, identita

Entita v obecném významu představuje jakýkoli objekt. Ve světě informatiky ještě přidáváme fakt, že je tento objekt zachycen v datovém modelu. Základním pravidlem pro entitu je její jasná rozlišitelnost od ostatních entit a nezávislá existence na ostatních entitách.

V identity managementu, jak se shoduje vícero autorů, je entita považována za základní stavební jednotku. Entitou může být osoba, organizační jednotka či objekt oprávnění. Ke každé entitě se váže mnoho atributů, které ji detailněji popisují. Cílem atributů je, aby vznikl co možná nejvíce kompletní popis dané entity a aplikace navázané na IdM mohla tato data dále zpracovávat. Pro ukládání dat o entitách nejčastěji slouží nějaká z adresářových služeb, která je vhodná pro ukládání velkého množství strukturovaných dat, umožňující definovat vztahy mezi objekty a poskytující možnost manipulovat s těmito daty (Sikora 2003).

O identitě se ve svých studijních materiálech zmiňuje docent Staudek (Staudek 2006): „*Identita je kontextově specifický rys – vznik a respektované provozování univerzálního globálního poskytovatele identity není pravděpodobné a to ani v dlouhém výhledu.*“ A definuje časté chápání identity jako totožnost entity, respektive vyjádření entity vůči jiným entitám.

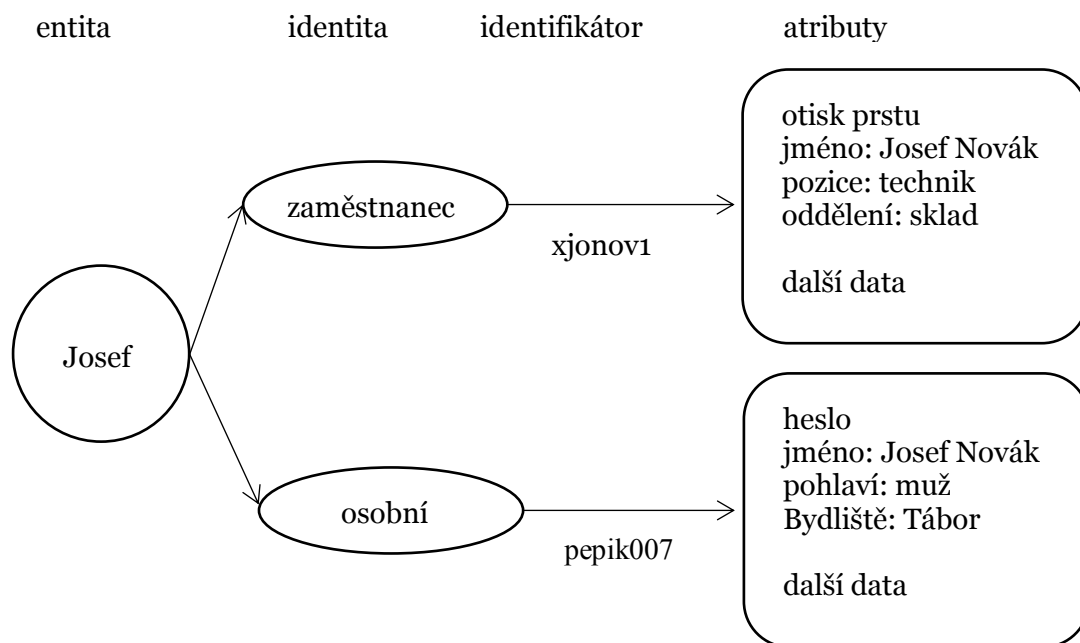
V informatice existuje několik všeobecně uznávaných standardů, které popisují i identity management. Vybral jsem v Evropě nejvíce využívaný, a tím je ISO standard, konkrétně ISO/IEC 24760–1, který definuje identitu jako množinu informací (atributů) reprezentujících entitu v ICT systémech. Účel ICT systému poté definuje, které z atributů popisujících entitu se používají pro identitu. Přičemž entita, může mít více než jednu identitu a několik entit může mít stejnou identitu. V určitých oblastech použití se identita může stát identifikátorem, který umožní entitám být v dané oblasti jednoznačně odlišenými (ISO/IEC 2011).

Na rozdíl od standardu ITU–T Y2720 (ITU-T 2009), ze kterého vychází autoři Bertino a Takahashi ve své knize (Bertino a Takahashi 2011), ISO standard pracuje pouze se dvěma typy dat, ze kterých se skládá identita:

- Identifikátor – jedinečný atribut nebo atributy identity (např. ID, e-mailová adresa, URI a IP adresa, telefonní číslo, číslo osobního dokladu).

- Atributy – slouží k charakteristice entit. Označují stav, vzhled nebo jiné vlastnosti entity (např. jméno, adresa, vzdělání, pracovní pozice).

ITU standard ještě používá autorizační údaje (pověření), tedy data dokazující nárok na danou identitu (např. otisk prstu, sken sítnice, digitální podpis). ISO tato data zahrnuje mezi atributy.



Obrázek 1 Vztah entita – identita – identifikátor – atribut (vlastní zpracování)

Vztahy mezi jednotlivými pojmy naznačuje Obrázek 1. Entita Josef má dvě rozdílné identity. Jednou je zaměstnanec a druhou osobní identita. Identifikátorem pro identitu zaměstnance je uživatelské jméno. Autentizace probíhá přes atribut otisk prstu. Identitě náleží i další atributy jako například jméno, pozice či oddělení. Josefově osobní identitě slouží jako identifikátor přezdívk. Autentizace probíhá přes atribut heslo. Dalšími atributy jsou například jméno, pohlaví, bydliště a další.

S identitou se také pojí její ochrana a riziko zneužití nebo krádeže. Pojem právo na soukromí (Gealfow 2016) je právě v dnešní době velmi aktuální. Považuje se za jedno ze základních lidských práv, kterého se ale na druhou stranu samotní uživatelé často dobrovolně, někdy nevědomky, vzdávají. Přesto, z hlediska uživatele i společnosti, je ochrana soukromí důležitá, a proto je také nedílnou součástí řízení identit. Problém spojený s digitálními identitami je, že neexistuje jednotný přístup k jejich vytváření ani správě. Hrozí nebezpečí krádeže identity, a tak je nutné prokazovat, že digitální identita je opravdu tou identitou, za kterou se vydává. Oblast digitálních identit přináší mnohá bezpečnostní rizika, kterým je třeba čelit s maximální snahou o eliminaci nebo minimalizaci hrozeb.

2.2 Životní cyklus identity

Osobně mi přijde nejvhodnější procedurální pohled na životní cyklus identity (Techopedia 2019). Obsahuje celý životní cyklus identity. Tedy fáze od jejího vzniku, přes správu identity a jejích přístupů, až po archivaci a odstranění. Identity management kontroluje celý proces přístupu k informacím a má poskytovat univerzální a konzistentní pravidla pro komplexní systémy a velký počet uživatelů. Z toho důvodu je pro úspěšné a praktické zavedení potřeba životní cyklus identity vhodně a detailně popsat, včetně všech procesů a možných stavů.

Životní cyklus identity obecně nemá pevně definované fáze, a tak si ho v detailu definuje každá společnost individuálně. Přesto se většina autorů shoduje na několika základních etapách, velmi podobných jakémukoli životnímu cyklu, které je možné následně dle potřeb různě rozšiřovat.

Například, zde již uváděný standard ISO (ISO/IEC 2011) zavádí pět základních etap:

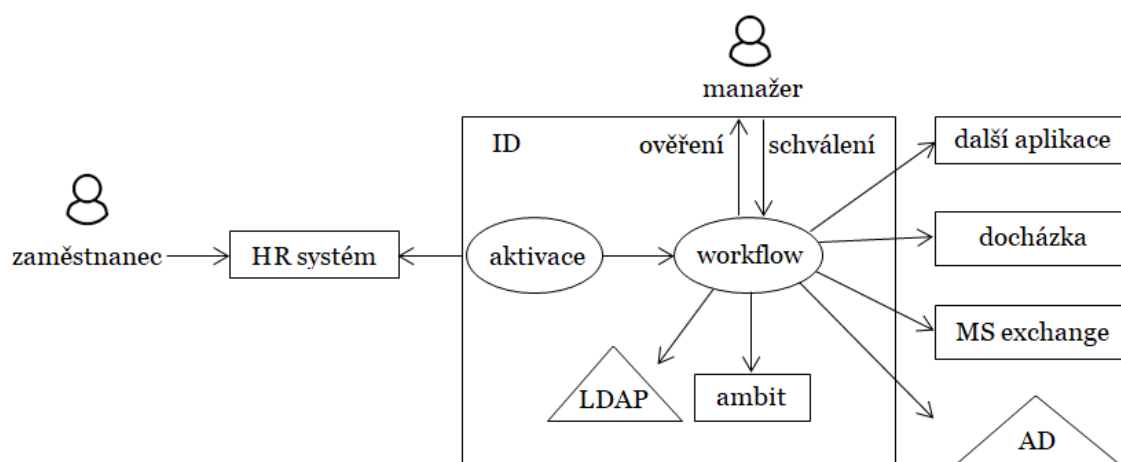
- Neznámá – nejsou známy žádné informace k identifikaci entity.
- Založená – základní požadované údaje o identitě, jejich ověření a následné založení identity.
- Aktivní – informace o identitě jsou zavedeny v identity managementu, zahájení interakce s dostupnými službami nástroji a zdroji, řízení a správa identity v průběhu jejího života.
- Blokována – informace o identitě jsou uloženy v identity managementu, ale entitě není umožněno využívat dostupné služby, nástroje a zdroje.
- Archivovaná – informace o identitě entity jsou stále přítomny, přestože entita již neexistuje. Informace nejsou nijak dostupné, pouze v případě obnovení entity.

Výhoda zavedení kvalitního životního cyklu identit tedy spočívá v tom, že každá identita se nachází v určité konkrétně popsané etapě životního cyklu a změny stavu jsou jasně definovány a popsány.

2.3 Workflow

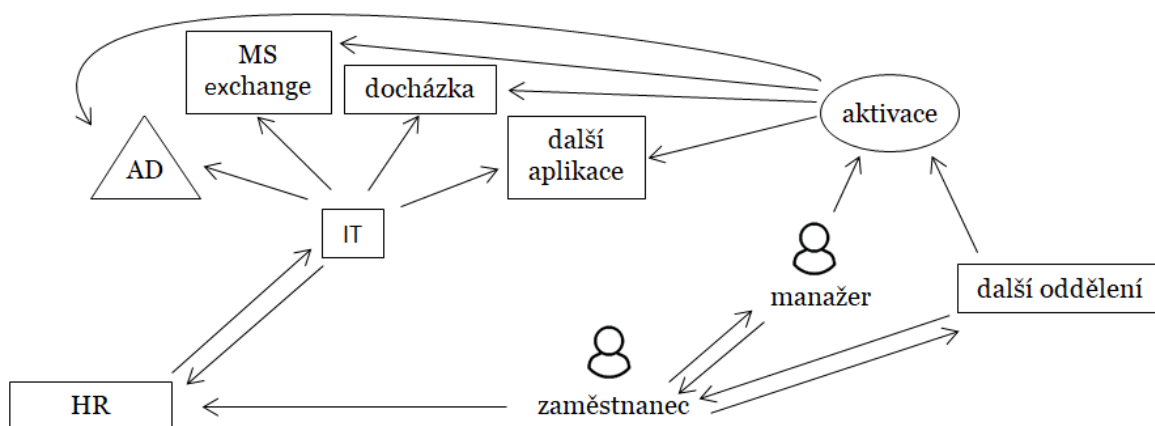
Workflow neboli pracovní postup obecně představuje rozpad komplexní činnosti na sekvenci jednodušších činností a vazeb mezi nimi. Nastavení a automatické spuštění definovaných kroků na základě určité definované akce. Jedná se o poměrně široký pojem.

Pro naši potřebu si pod workflow představujeme postup, který automatizuje tok informací, dokumentů a procesů napříč společnostmi. Hlavní pozornost je věnována procesu, nikoli předávanému obsahu. Tedy tomu, jak daný obsah postupuje společností (Walker 2003). V identity managementu je hlavním cílem nastavení správných přístupů a oprávnění identitám.



Obrázek 2 Příklad možného workflow při nástupu zaměstnance (Vohnoutová 2008; vlastní zpracování)

Příkladem jednoho z možných workflow při vzniku identity může být nástup nového zaměstnance, který popisuje Obrázek 2. Jeho cesta společností začíná požadavkem na nástup nového zaměstnance, který zadá personální oddělení nebo nadřízený. Poté by měl již následovat automatizovaný proces. Identity management zjistí nový nástup v systému. Vytvoří a nastaví účet zaměstnance se všemi požadovanými parametry a přístupy. Pokud je třeba, inicializuje proces schválení a po něm účty aktivuje (Active Directory, email, aplikace, ...). Celý proces je auditován.

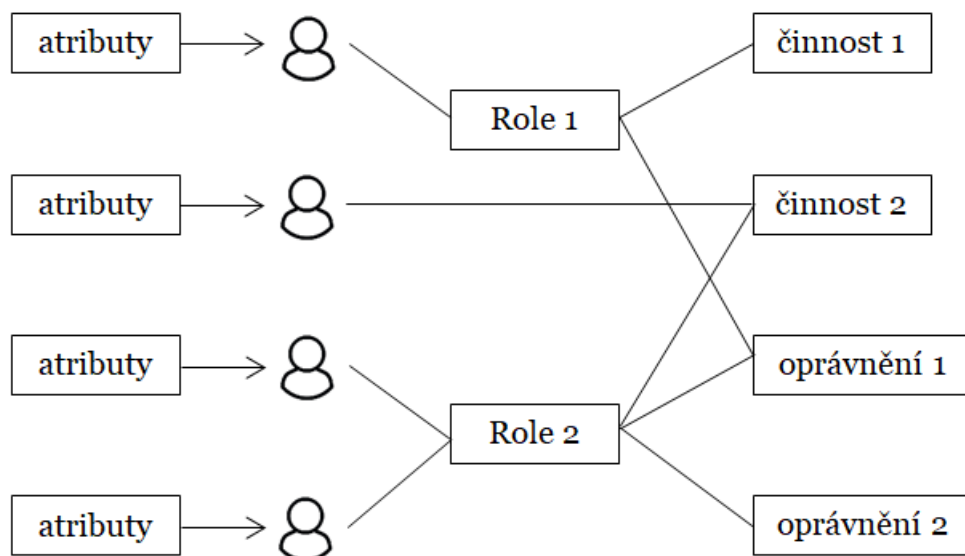


Obrázek 3 Možný nástup zaměstnance bez zavedeného workflow (vlastní zpracování)

Jak by stejný proces vypadal bez implementovaného IdM řešení a zvládnutého workflow ukazuje Obrázek 3. Nejenom, že se doba celého zpracování může výrazně prodloužit (čekání na jednotlivé schválení a nastavení), ale představuje mnohdy nepříjemné kolečko nového zaměstnance po společnosti.

2.4 Tvorba a správa identit

Cílem každého identity management řešení je sjednocení všech identit, jejich účtů a eliminace rozdílů ve správě jednotlivých systémů. Identita v rámci systému musí obsahovat předem definované atributy (např. jméno, příjmení, pozice), a dále může obsahovat i nepovinné nebo doplňující informace (např. telefonní číslo). K identitě se také přiřazují určité skupiny oprávnění, vztahující se k určité pozici nebo činnosti, tzv. role, jak popisuje Obrázek 4.



Obrázek 4 Vztah mezi identitou a rolemi (vlastní zpracování)

Takto centralizovaná správa umožňuje administrátorům kontrolovat zařízení, která do sítě společnosti vstupují. Za druh identity mohou být tedy považovány také notebooky, smartphony, tablety a další zařízení. Je možné jim nastavit přístupová oprávnění stejně, jako by se jednalo o skutečné osoby. I v tomto případě lze pomocí IdM vynutit dodržování pravidel, bezpečnostních politik společnosti a udržovat tak nad zařízeními dostatečný přehled (Waters 2018).

Níže je uvedeno několik příkladů identit:

- Nový zaměstnanec – v IdM je mu vytvořena identita odpovídající pracovní pozici s příslušnými právy. Pokud nadřízený vyžaduje nějaká oprávnění nad rámec výchozí role, musí jejich přidělení projít schvalovacím procesem.
- Externí dodavatel – v IdM je vytvořen účet s přístupem pouze do systému, kvůli kterému byl najat. Po uplynutí stanoveného termínu je účet automaticky deaktivován, prodloužit jej může pouze v dané společnosti pověřená osoba, nebo je účet úplně zrušen.
- Notebook – v IdM je vytvořen účet s přístupem do interní wifi sítě.
- Docházkový systém – v IdM je veden jako bezpečnostní prvek a je mu dovolen přístup na server pro ukládání záznamů o docházce zaměstnanců.

Důvodů ke správě identit je celá řada (Krejčí 2008):

- Neplatné přístupy – odchod zaměstnance, a s tím související zrušení jeho digitální identity, málokdy probíhá podle nějakého procesu. Účty jsou buď využívány někým jiným, anebo se jen prostě zapomene na IT nahlásit odchod uživatel k zablokování.
- Oprávněnost přístupu – ne vždy společnost udržuje mapu pracovních pozic a ještě méně často s nimi související oprávnění. O jejich přidělení často rozhoduje nadřízený, a to ještě ad-hoc v rámci nějakého urgentního požadavku. Navíc nejde očekávat, že manažer oddělení má přesný přehled o všech možnostech přístupu do mnoha aplikací, které jeho oddělení používá.
- Kumulace přístupů – obvyklý jev spojený se změnou pracovní pozice v rámci společnosti. Málokdy se řeší s přechodem na novou pozici kompletní odebrání přístupů do systémů, se kterými již uživatel nepracuje.
- Kvalitní audit – IdM přináší možnost auditovat chování uživatele v celém prostředí, nejen v oddělených aplikacích, což přináší komplexní přehled pro vedoucí pracovníky, a tedy i snazší korekci svých podřízených.

2.5 Autentizace a autorizace

Autentizace představuje proces ověření pravosti identity na základě předložených údajů. Jde o bezpečnostní opatření, sloužící k ochraně dat a před falšováním identity. Nejedná se o nic jiného, než o propojení osoby používající určitou aplikaci nebo systém y odpovídající digitální identitou. Autentizace jednoduše říká, že osoba zadala správné údaje k potvrzení vlastnictví digitální identity. To danou osobu ale ještě neopravňuje aplikaci nebo systém používat. To má na starost autorizace, která je dále zmíněna v průběhu kapitoly. Autentizaci dnes v digitálním světě používá téměř každý, často i několikrát denně. Používá se pro přístup k e-mailovému účtu, počítači, síťovému uložšti a desítkám dalších systémů a služeb (Moore 2014).

Slabým článkem autentizace může být uživatel a jeho pohodlí. Pokud by byla jen na něm, ideálně by se obešel úplně bez ní nebo ji alespoň co nejvíce zjednodušil, tedy například na používání hesla: heslo. Proto zodpovědní administrátoři přicházejí s opakujícími se restrikcemi na nová hesla o určitém minimálním počtu znaků, specifickém symbolu a číslech. Případně zavádějí vícefaktorové ověření. Uživatelsky vítanou, a přitom stále bezpečnou možností ověření, může být zavedení SSO (Single Sign-On) autentizace, která ve zkratce umožňuje uživatelům zadávat uživatelské jméno a heslo jedinému systému, přes který zůstává po určitou dobu přihlášen na všech systémech, které jsou k SSO napojeny bez nutnosti opětovného ověřování.

Základní metody autentizace (Požár 2005):

- Podle toho, co uživatel zná (jméno a heslo nebo PIN, gesto na obrazovce telefonu, atd...). Nejčastěji používaná metoda, označovaná za jednofaktorovou autentizaci.
- Podle toho, co uživatel má (technický prostředek – hardwarový klíč, smart card, privátní klíč, ...).

- Podle toho, čím uživatel je (biometrické ověření – otisk prstu, rozpoznání obličeje, snímek sítnice...).

Autentizace může, pomocí kombinací metod, probíhat na základě více údajů. Poté se jedná o vícefaktorovou identifikaci, která se v případě kombinace dvou metod nazývá dvoufaktorová a v případě kombinace tří metod, třífaktorová. Příkladem vícefaktorové autentizace je uživatel, který se do aplikace přihlásí pomocí svého uživatelského jména a hesla. Následně mu je doručen jednorázový PIN kód na mobilní telefon, který zadá do aplikace a finálně se přihlásí. Tím je uživatel ověřen více faktory (Gašpařík 2018).

Po autentizaci probíhá autorizace, která zjišťuje, zda má uživatel nárok přístupu do systému, aplikace, k souboru. Ví tedy, na co má přihlašovaná identita oprávnění a podle toho přístup buď povolí, nebo zamítne.

Systémy a aplikace často mají svůj vlastní způsob autorizace, což znamená, že pro každý uživatelský účet, který zaměstnanec používá, existuje vlastní struktura oprávnění a způsob nastavení.

Způsoby autorizace (IDMWORKS 2015):

- Hodnota atributu – přístup uživateli je povolen nebo zamítnut na základě hodnoty uživatelských atributů.
- Role – o přístupu je rozhodováno na základě informací o uživateli neboli přiřazení role, skupiny (např. oddělení, pozice, lokalita, projekt, atd...).

2.6 Logování a audit

Možnosti logování a auditu činí IdM řešení efektivnější. Centralizovaný systém přihlašování vede k možnosti vytváření záznamů (tzv. logů) o aktivitách identit. Lze také sledovat chování identity v systému po autorizaci – jak pracuje, jaké programy spouští, apod. Potřebné informace (kdo, co a kdy) se zaznamenávají do databáze a je možné je dále zpracovávat.

Logování obecně označuje činnost, při níž systém vytváří záznamy (tzv. logy), do kterých jsou ukládána data za účelem pozdější analýzy. Přínosy logů jsou jak statistické, jako počty přihlášení nebo způsob používání systému, tak také slouží ke splnění požadavků na odpovědnost, přispívají k ochraně osobních informací, k jednoznačnému přiřazení odpovědnosti uživatele a jeho činů, k optimalizaci systémů, zefektivnění práce, objevení chyb a poskytuje oznámení odpovědným entitám.

Pojem audit definuje Český slovník kybernetické bezpečnosti jako (Jirásek et al. 2015): „*Systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna.*“

Dále slovník říká, že auditovaná událost je (Jirásek et al. 2015) „*systémem detekovaná akce, která vyvolá spuštění auditu.*“ A posledním pojmem je auditní záznam (Jirásek et al. 2015): „*Chronologický zápis aktivit v systému, které jsou dostatečné pro rekonstrukci,*

zpětné sledování a vyhodnocení sekvence stavu prostředí a aktivit souvisejících s operacemi a procedurami od jejich počátku ke konečnému výsledku.“

Auditní záznam tedy vytváříme proto, aby z něj bylo možné přesně identifikovat nedovolené i dovozené akce uživatele. Obsahuje přesný čas, informace o uživateli, ovlivněných systémech a prováděných akcích. Výstupy auditních záznamů se dnes zpracovávají pomocí specializovaných programů, které dokážou upozornit na co se zaměřit a ulehčit jejich analýzu. Dokonce některé pokročilé systémy jsou do jisté míry schopné sami provést automatickou analýzu záznamů (Požár 2005).

Audit může probíhat jak interně, tak i externě. Pro interní účely je možné auditní služby využívat k automatickému vytváření varování podle informací z logovacích záznamů. Například opakované neúspěšné přihlášení do systému. Pro účely externího auditu, služba poskytuje na základě logovacích záznamů přesné a rychlé podklady, nejenom bezpečnostního charakteru.

Pokyny pro logování a audit dle ITU standardu (ITU-T 2009) zahrnují:

- Logování a auditování událostí souvisejících s IdM (např. přístup k informacím o identitách, neoprávněný pokus o přístup, aktualizace časových značek, atd.) pro forenzní analýzu.
- Zpětné sledování provedených operací.
- Detekce nesouladu s nastavenými politikami.
- Zajištění interních a legislativních požadavků.

2.7 Integrace

Vzhledem k povaze zaměření identity managementu, tedy správě identity, je jedním z jeho hlavních cílů držet informace o identitách na jednom místě napříč co největším počtem systémů. O identity managementu můžeme mluvit jako o integračním systému. Měl by být schopen propojit různé databáze, adresářové systémy a aplikace, které společnost využívá jako například CRM, HR systém, docházku, a další. To poté může vést k efektivní administraci a minimalizaci duplicitních dat.

Integrace systémů může probíhat buď tak, že se databáze s uživatelskými informacemi z různých systémů sjednotí do jedné databáze spravované identity managementem, nebo se využívá tzv. konektorů, které zajišťují výměnu požadovaných informací mezi databázemi určitého systému a identity managementem.

Konektor je malá programová komponenta, jejímž úkolem je zajistit komunikaci (výměnu dat) mezi konektorovým rozhraním IdM systému (SPI) a komunikačním rozhraním cílového systému a delegovat operace pro správu na tyto systémy. Vytvoření konektoru obecně bývá relativně jednoduchá záležitost. Většinou neobsahuje složitou logiku a přizpůsobuje se napojenému systému, v němž tak nebývá potřeba dělat úpravy, a to celý proces zjednodušuje. Například nastavení e-mailové adresy v určitém systému – úkolem konektoru není vygenerování adresy, to je práce pro IdM systém, konektor pouze zajistí přenesení informace o e-mailové adrese do cílového systému (Semančík et al. 2015).

Přesto právě tvorba jednotlivých konektorů je často velmi významná položka v rozpočtu celého IdM řešení.

Konektory obecně poskytují základní metody pro (Cirkva 2018):

- Vytvoření nového uživatelského účtu, popř. skupiny, role, organizace apod.
- Editaci stávajícího uživatelského účtu.
- Smazání uživatelského účtu.
- Vyhledání účtů.

Konektory se dělí na dva typy (Vohnoutová 2008):

- Proprietární – aplikace jsou integrovány pomocí konektorů, které je potřeba nejprve naprogramovat a nejsou kompatibilní mezi různými IdM systémy. Příkladem může být HR systém společnosti, požadavkový systém, apod.
- Celosvětově rozšířené aplikace – existuje pro ně standardizovaný konektor, s nímž jsou dodávány. Příkladem takových aplikací a systémů jsou mimo jiné: SAP, JIRA, Oracle, RedHat Linux, MySQL, MS IIS, Dropbox, Office 365 a další.

Složitost integrace je individuální a vždy se odvíjí od komplikovanosti a unikátnosti řešení v dané společnosti. Většinou ale platí, že čím více dat je třeba integrovat, tím je proces složitější.

2.8 Samoobsluha

Jedním z velkých a viditelných benefitů IdM řešení přímo pro uživatele je, kromě obecně rychlejšího zpracování požadavků vztahujících se k uživatelským identitám, možnost uživatelské samoobsluhy některých požadavků, které do doby zavedení IdM řešení musí zpracovávat IT podpora, což v mnohých případech může být zdlouhavé. Různé studie uvádí, že cena resetování hesla uživatele IT podporou vychází na vyšší desítky dolarů, přičemž klidně více než 20 % z celkového počtu požadavků na IT podporu je právě změna hesla (Shankar 2016).

Takovým typickým požadavkem bývá například změna hesla do koncového systému. V případě IdM řešení s uživatelskou samoobsluhou si uživatel může přes webové rozhraní jednoduše a během pár minut změnit heslo sám.

Samoobsluha může mít podobu samostatného webového rozhraní nebo může být navázána na stávající požadavkový systém, který společnost používá. Také míra pravomocí uživatele – úplná změna, změna vyžadující schválení nadřízeného či zodpovědné osoby nebo kombinace obou možností podle významnosti systému, je nastavována individuálně, dle požadavků konkrétní společnosti a používaných systémů.

3 Implementace IdM do prostředí reálné společnosti

Následující část práce bude pojednávat o samostatné implementaci řešení identity managementu do prostředí reálné společnosti ALD Automotive s.r.o.

Kapitola nekomentuje konfiguraci v celém jejím rozsahu, ani se nejedná o instalační dokumentaci. To by ani vzhledem k nutnosti individuálního přístupu ke každému nasazení nebylo dost možné. Naopak cílem je obecně popsat celý průběh a přístup k implementaci řešení identity managementu, který by měl být využitelný i při dalších nasazeních.

Jednotlivé podkapitoly korespondují s průběhem implementace od prvotního nápadu, definici požadavků, výběr dodavatele, až po konfiguraci funkčního řešení.

3.1 Analýza současného stavu

Společnost ALD Automotive s.r.o. je poskytovatel operativního leasingu pro osobní a lehké užitkové automobily. Spravuje více než 23 000 vozidel a patří ve svém oboru mezi největší společnosti. Je součástí skupiny mateřské společnosti Sociétés Générales a je sesterskou společností Komerční banky. Klienty společnosti jsou soukromé osoby, drobní živnostníci, ale především firmy a velké nadnárodní korporace, o které se společnost stará na globální úrovni.

Společnost v Čechách čítá okolo 150 zaměstnanců, z nichž několik je zaměstnáno na částečný úvazek. IT oddělení eviduje i 3 externí zaměstnance a 74 dodavatelů, kteří mají přístup do systémů společnosti. Centrála čítající většinu zaměstnanců se nachází v Praze. Centrum ojetých vozů sídlí ve Zdíbech u Prahy. Dále má společnost ještě dalších pět poboček, a to v Ústí nad Labem, Plzni, Českých Budějovicích, Brně a Ostravě.

Propojení se sesterskou respektive mateřskou společností mimo jiné znamená, že IT infrastruktura společnosti je v poměrně velké míře integrována právě do infrastruktury mateřské potažmo sesterské společnosti. Což sebou nese určitá omezení a nutnost podřídit se v mnohých rozhodnutích pokynům shora.

Síťová infrastruktura je postavena na virtualizačním prostředí VMware, čítající momentálně 79 virtuálních serverů, jejichž provoz zajišťují 3 fyzické hypervisor servery. Používány jsou jak operační systémy Windows Server, tak i různé Unix/Linux distribuce. K záloze dat je využíván jeden fyzický backup server. Pro zajištění obnovy chodu existuje odloučená disaster recovery (DR) lokalita, tvořena jedním fyzickým DR serverem.

Vstupní informace o identitách poskytuje požadavkový systém ServiceDesk, do kterého vedoucí oddělení zadávají požadavky na nástup, odchod, či změnu identity nebo jejich atributů a oprávnění. Oddělení lidských zdrojů (HR) společnost přímo nemá. Služby HR

oddělení jsou poskytovány sesterskou společností a do HR systému tak společnost nemá žádný přístup. To je jeden z důvodů, proč do této doby neexistuje prakticky žádná automatizace, a všechny kroky spojené s identitami jsou odpovědností vedoucích pracovníků, od nichž také vždy musejí vzejít nebo alespoň získat jejich schválení.

Vznik identity začíná příchodem požadavkem do ServiceDesku, kam ho zadá vedoucí pracovník nového zaměstnance. Zde ho přebírá ke zpracování pracovník infrastrukturní části IT oddělení. Zkontroluje, zda jsou vyplněny všechny potřebné informace k založení identity. Pokud ne, kontaktuje vedoucího s žádostí o doplnění informací. Pokud ano, založí uživatele v Active Directory (AD) dle pravidel společnosti a přiřadí mu příslušná oprávnění vzhledem k jeho pozici, případně požadavkům nadřízeného. Následně nové identitě vytvoří e-mailovou schránku na Exchange serveru, vytvoří přístup k síťovým tiskárnám používající nástroj SafeQ a jako poslední krok zaeviduje nového uživatele do aplikace spravující majetek společnosti. Případně vyřeší speciální požadavky vztahující se k infrastruktuře jako je nákup nového zařízení či množnost pracovat vzdáleně z domova. Na závěr pošle vedoucímu informační e-mail o vytvoření a základní konfiguraci nového účtu, případně o stavu požadavků nad rámec běžného nástupu zaměstnance. Poté vrátí požadavek operátorovi aplikační podpory, jenž identitě přiřadí požadované aplikační přístupy a po informování vedoucího požadavek uzavírá.

Při jakékoli úpravě identity je požadavek opět vytvořen v ServiceDesku. Ten si následně, dle charakteru požadavku, přebírá buď operátor infrastruktury, nebo aplikační podpory. Pokud se jedná o úpravu, která podléhá schválení, kontaktuje operátor zodpovědnou osobu. Po vyřešení požadavku operátor opět informuje uživatele a požadavek uzavírá.

Zánik identity musí vzejít od nadřízeného, který jej musí opět nahlásit do ServiceDesku. Postupně se provedou stejné kroky jako v případě vzniku identity, akorát s tím rozdílem, že tentokrát dochází k mazání a blokování přístupů, případně přesměrování na jiné identity.

Jednou z hlavních motivací implementace řešení identity managementu byl rostoucí počet požadavků vztahujících se ke správě identit a bezpečnostní riziko spojené s nenahlášenými odchody zaměstnanců, a tím vznikající tzv. „mrtvé duše“.

V době zahájení projektu bylo spravováno 180 uživatelských účtů, 68 dodavatelských účtů a dále desítky účtů pro přístup externí společnosti do systému správy pohledávek. Ke správě účtů je využíváno Microsoft LDAP (Lightweight Directory Access Protocol) adresářové služby Active Directory. Společnost používá několik externích systémů, které budou nadále spravovány ručně, mimo správu IdM řešení. Spravováno bylo celkem 34 systémů, na některých z nich je zavedena autentizace pomocí SSO.

IT oddělení v době vzniku myšlenky zavedení identity managementu mělo následující strukturu:

- **Infrastruktura** – čítající 4 členy a spravující IT infrastrukturu společnosti. Zajišťuje dodávky IT technologií, spravuje počítačovou síť a síťové zdroje, zajišťuje bezpečnost a poradenství na úrovni obecných systémů a hardwaru.

- Aplikace – čítající 4 členy úzce spolupracující s projektovým oddělením. Zajišťuje chod a vývoj interních aplikací a řešení s nimi spojených problémů.

3.2 Definice požadavků

Před prvním kontaktem s možnými dodavateli bylo nutné definovat základní požadavky na funkčnost řešení identity managementu. Vzhledem k tomu, že žádný ze zaměstnanců IT oddělení společnosti neměl praktické zkušenosti s takovým řešením, byly řešitelným týmem, jehož členem byl také autor, stanoveny i obecnější požadavky. Ty vzešly z rešerše produktů na trhu, které autor představil zbytku týmu a následného týmového brainstormingu o funkčnosti řešení. Definované požadavky vycházejí z potřeb společnosti, které zahrnují automatické odbavení rutinních požadavků, snazší administraci účtů, konzistentnost nastavení, posílení bezpečnosti, určení zodpovědnosti, získání podkladů pro audit, zjednodušení a urychlení řešení uživatelských problémů. Vzniklý seznam požadavků byl následně rozeslán možným dodavatelům, v následujícím rozsahu:

Body 1–3 byly považovány za nutnost. Body 4–6 považovány za vhodné implementace. Body 7–10 spíše dotazy, zda je v rámci IdM řešení něco takového možné.

- 1) Automatizace častých úloh (vytvoření, změna, smazání účtu, změna hesla).
- 2) Automatizace schvalovacího procesu – nástup a odchod zaměstnance, přidělení a odebrání práv, změna pracovní pozice.
- 3) Auditovatelnost.
- 4) Samoobsluha uživatelů (změna hesla, žádost o přístup či oprávnění).
- 5) Propojení s aplikačními systémy (docházka, tisk, účetní systém, systém pro správu dokumentů a další interní aplikace).
- 6) Možnost správy File Share oprávnění.
- 7) Inventura rolí – report nadřazenému, které role má zaměstnanec přidělené. Možnost rychlé, uživatelsky přívětivé kontroly a případné úpravy.
- 8) Řízení oprávnění v systémech a aplikacích – správa přístupu pro externí subjekty.
- 9) Exkluzivita rolí a oprávnění – například účetní nemůže vydávat faktury a současně faktury kontrolovat.
- 10) Kontrola bezpečnostních incidentů – například jeden účet použit na více lokalitách ve stejnou dobu.

Dále bylo ujasněno, že pro společnost není nezbytné, aby všechny funkce byly okamžitě nasazeny. Spíše by se mělo jednat o postupný a přírůstkový průběh implementace. Začít od základních stavebních prvků IdM řešení a průběžně přidávat další funkcionalitu.

Pro výběr dodavatele byla za nutnou podmínku stanovena možnost lokální podpory. Výhodou bylo použití open source nástroje.

Hodnotící kritéria byla stanovena (řazeno od nejvyšší priority):

- Splnění bodů poptávky 1–3.
- Splnění zbylých bodů poptávky.
- Cena instalace a implementace.

- Cena technické podpory na 1 rok.
- Sazba za 1 Man-day (MD).
- Unikátní funkcionalita.

3.3 Výběr řešení

Následujícím úkolem autora, po vydefinování základních požadavků a očekávání na řešení identity managementu, bylo provést rešerši možných dodavatelů a jejich následné oslovení. Vybrané společnosti byly osloveny s definovanými požadavky, které jsou popsány v předchozí kapitole 3.2 a byl s nimi veden úvodní telefonický hovor nebo schůzka. Výstupy schůzek byly prezentovány vedení IT oddělení a následně byly vybrány společnosti do interního výběrového řízení, po jehož zpracování a vyhodnocení vzešlo finální řešení. Dále kapitola stručně představuje vybraný nástroj pro řešení identity managementu a implementátora.

3.3.1 Rešerše možných dodavatelů

Vybrány a osloveny byly následující společnosti:

- Onlio, a.s. s řešením JIRA Crown
 - Produkt nesplňuje požadavky, a tím pádem automaticky vypadl po prvním kontaktu z množiny možných řešení.
- Orchitech Solution, s.r.o.
 - Soulad s požadavky – ano. U kontroly bezpečnostních incidentů odlišují terminologii Identity a Access management. Pravděpodobně nutný zásah do interních systémů při napojení.
 - Součást komunity OpenIDM, open source produkt Wren:IDM.
 - Řešení jako skládačka – klient si vybere, co potřebuje.
- BCV Solution s.r.o.
 - Soulad s požadavky – ano, plně.
 - Vlastní produkt CzechIdM. Nutné mít zakoupenout maintenance.
 - Pokrývá všechny oblasti řešení. Velká funkcionalita.
- AMI Praha a.s.
 - Soulad s požadavky – ano, plně. Nedoporučují File share řešení.
 - Neomezují se na jeden produkt, nabízí proprietární i open-source řešení. Doporučují open-source Evolveum midPoint.
 - Nabízí vlastní cloudové řešení IdM jako služby – SkyIdentity.
 - Řešení zahrnuje i bezpečnostní prvky.
 - Placená analýza před finální nabídkou.
- Alloy s.r.o.
 - Soulad s požadavky – ano, plně.
 - Vlastní proprietární produkt EasyIDM založený na Microsoft Identity Manager.

- GAPP System, spol. s.r.o.
 - Soulad s požadavky – ano, plně.
 - Open source produkt Evolveum midPoint.
 - Řešení zahrnuje i bezpečnostní prvky.
 - Dodavatel, se kterým již společnost spolupracuje na jiných projektech.

Na základě informací a schůzek s oslovenými dodavateli byly pro interní výběrové řízení a vyžádání cenové nabídky vybrány 3 společnosti – GAPP System, spol. s.r.o., AMI Praha a.s. a Alloy s.r.o.

Společnosti Orchitech Solution, s.r.o. a BVC Solution s.r.o. nebyly k dalšímu jednání přizvány převážně z důvodu preference jiného produktového řešení, než pro které se společnost po prvním kole schůzek rozhodla. Dále u společnosti Orchitech Solution byly ve větším měřítku očekávány nutné zásahy do stávajících systémů a u společnosti BVC Solution bylo potřeba počítat s povinnými náklady na údržbu. Také komunikace již prakticky od začátku jednání neprobíhala tak, jak by si společnost představovala. Výsledek výběrového řízení shrnuje Tabulka 1 níže.

Tabulka 1 Interní výběrové řízení na dodavatele (vlastní zpracování)

	GAPP Systém	#	AMI	#	Alloy	#
Splnění bodů poptávky 1–3	Ano	1	Ano	1	Ano	1
Splnění zbylých bodů poptávky	Ano	1	Ano	1	Ano	1
Cena instalace a implementace	180 000 Kč	1	840 000 Kč	3	288 000 Kč	2
Cena technické podpory na 1 rok	38 000 Kč	1	240 000 Kč	3	67 650 Kč	2
Sazba za 1 MD	14 400 Kč	3	12 000 Kč	1	12 000 Kč	1
Unikátní funkcionalita	Ověřené řešení	–	Cloud služba	–	–	–
Výslední pořadí	1.		2.		3.	

Vybranou společností, která se podílela na zavedení identity managementu, se tedy stala společnost GAPP System, spol. s.r.o. Nasazovaným řešením bude open source produkt Evolveum midPoint, upravený pro potřeby společnosti.

3.3.2 Evolveum midPoint

Slovenská Společnost Evolveum vznikla v roce 2011 odštěpením od projektu OpenIDM a založila vlastní projekt IdM řešení MidPoint (Semančík 2018b). Společnost se opírá o více než patnáctiletou zkušenost v oblasti identity managementu. Jedná se o open source produkt, snadno modifikovatelný, pracující na bázi komponent (Evolveum 2018a). Společnost sama svůj produkt charakterizuje jako základní stavební blok, ze kterého se následně buduje pokaždé jedinečné řešení. Zaměřuje se nejen na správu a zabezpečení identit, ale také na řízení přístupu (Evolveum 2018c).

Šest základních stavebních funkcí (Evolueum 2018c):

- **Správa identit** – umožňuje definovat, vynutit a kontrolovat bezpečnostní politiky a přístupová práva v oblasti identit a výměny dat mezi interními i externími systémy. Pokrývá celý průběh správy životního cyklu identity a zajišťuje konzistenci mezi všemi právy a bezpečnostními politikami společnosti. Podporuje různé kontroly přístupu, jako je správné přiřazení rolí uživatelům nebo audit, což vede ke snižování rizik, ovlivňujících výkonnost podniku a napomáhá udržení vysokého standartu bezpečnosti.
- **Audit** – poskytuje zpětnou vazbu k důležitým akcím a událostem v systému, jako například kdo požaduje přístup, proč byl přístup povolen nebo zamítnut, kdo jej schválil. Z auditních záznamů by mělo být možné „vrátit se v čase“ a rekonstruovat stav systému v minulosti. V době vzniku této práce bylo možné provádět auditování do logovacích souborů a databázových tabulek.
- **Organizační struktura** – podpora flexibilní organizační struktury, nevyžaduje striktně hierarchické stromové struktury. Může se skládat z objektů, jako jsou divize, oddělení, týmy, projekt, apod. Objekt není nijak omezován, může mít jednoho nebo více rodičů a struktury mohou být i vícenásobné. Organizační struktura se většinou váže ke struktuře rolí, kde poté uživatelé patřící pod určitý objekt mají stejnou roli. Každý objekt je také současně rolí. Pokud je tedy tomuto objektu přiřazen uživatel, chová se stejně jako role a automaticky provede všechna odpovídající přiřazení a nastavení.
- **Správa přihlašovacích údajů** – hesla mohou být držena a spravována přímo v IdM řešení. V tom případě je možné přímo vytvářet hesla jak pro uživatele, tak pro zdroje a během jejich celého životního cyklu se o ně starat. Samozřejmostí je možnost definovat vlastní zásady pro tvorbu hesel – jaké znaky budou povoleny nebo naopak zakázány, délka hesla, jedinečné znaky, počet znaků, jejich opakování, použití velkých a malých písmen, číslic a speciálních znaků.
- **Workflow** – zajišťuje provedení vybraných akcí (například přiřazení oprávnění) až po schválení příslušnými pověřenými osobami nebo rolemi. Uživatel získá přístup nebo informace až poté, co požadavek projde předem definovaný sled událostí. Workflow proces běžně zahrnuje tvorbu, úpravu, odstranění, povolení nebo zakázání.
- **Správa oprávnění** – specifikuje zdroje, ke kterým mají mít uživatelé na základě příslušnosti k určitým rolím přístup. Využívá se tedy tzv. oprávnění založené na roli (Role-base access control, zkratka RBAC). Určuje, co mohou uživatelé dělat po vstupu do aplikace nebo sítě. Vzniká soulad mezi uživateli, rolemi a zdroji, což přináší větší míru zabezpečení.

Společnost se také zabývá otázkou GDPR. Vzhledem k tomu, že IdM řešení pomáhá společnosti mimo jiné zmapovat procesy, vyčistit data a nastavit správné politiky, týká se i osobních údajů a dat. IdM může spravovat osobní data nejenom zaměstnanců, ale také dodavatelů či klientů, a právě proto jsou IdM řešení vhodná jako správci záznamů a podpora pro GDPR. MidPoint díky tomu, že zaznamenává data o operacích, ví co, kdy a jak se stalo. Také poskytuje informace, z jakého důvodu byla data o identitě zaznamenána a zpracována. MidPoint může udržovat záznamy o právních základech pro

zpracování dat. Jedním z nich je udělený souhlas o zpracování. Zná rozsah souhlasu a na jeho základě je schopen určit jaké účty je třeba smazat, které atributy upravit či vymazat a které služby odebrat. Může se tak starat o zpracování souhlasu i jeho odmítnutí nebo o žádosti na úpravu údajů či jejich vymazání. IdM řešení tak nabízí zajímavou možnost zajištění požadavků GDPR (Evolveum 2018b).

3.3.3 GAPP System spol, s.r.o.

Společnost GAPP System, spol. s r. o. sídlí v Praze a má již 25letou historii v oboru. Vizi společnost je (GAPP System 2014): „Zajistit spolehlivé, výkonné a bezpečné prostředí pro informační systémy a data našich zákazníků a tím přispět k jejich vlastnímu úspěchu.“

Orientuje se na provoz informačních systémů, datová centra, disaster recovery řešení, virtualizaci a datovou bezpečnost obecně. Mezi jejich klienty patří mimo jiné bankovní instituce, Český rozhlas, Nejvyšší kontrolní úřad, Ministerstvo financí ČR nebo O2. Ve společnosti ALD Automotive s.r.o. se již podíleli na modernizaci a konsolidaci IT infrastruktury se zabezpečením dat a vybudováním disaster recovery lokality.

3.4 Nasazení a konfigurace

Po výběru dodavatele bylo potřeba přistoupit k finálnímu stanovení rozsahu základní implementace, vyčlenění kapacit a následně zahájit samotnou realizaci.

Za ALD Automotive byli mimo autora vybráni další dva zaměstnanci k dohledu nad projektem, a to vedoucí infrastrukturní části IT a bezpečnostní manažer společnosti. Na straně dodavatele byla určena zodpovědná osoba za vedení projektu a jeden člověk mající zodpovědnost za průběh realizace.

Na zahajovací schůzce byl domluven rozsah základní implementace řešení identity managementu. Ten obsahuje následující body:

- Ze strany ALD Automotive:
 - Přípravu prostředí pro zavedení identity managementu.
 - Analýzu a definici uživatelských rolí, oprávnění a workflow nástupu uživatele. Tento bod představuje jeden z častých problémů během průběhu implementace IdM řešení, případně jeho následného provozu.
 - Vyčištění Active Directory – aktualizace organizačních jednotek, skupin a uživatelů. Odstranění mrtvých duší.
- Ze strany GAPP Systems:
 - Instalaci a konfiguraci IdM řešení midPoint na prostředí připravené zákazníkem.
 - Napojení Active Directory a automatizace vytváření, správy a mazání uživatelských účtů.
 - Zavedení samoobsluhy uživatelů.
 - Zaškolení správy IdM řešení midPoint.

- Společně:
 - Customizace midPoint řešení pro potřeby ALD Automotive.

Po dokončení této základní implementace a otestování provozu dojde k vyhodnocení fungování identity management řešení a případnému rozšiřování funkčnosti na další systémy spolu s prohlubováním automatizace.

3.4.1 Analýza skupin a identit

Cílem analýzy bylo určit tzv. business role, které by se v rámci identity managementu přiřazovaly jednotlivým identitám a obsahovaly příslušné skupiny z Active Directory (v IdM vedené jako role). Dále určit speciální oprávnění, které se nehodí zahrnovat pod konkrétní business role. O ty mohou identity žádat v samoobsluze IdM. Příkladem může být oprávnění barevného tisku.

Vstupní data pro analýzu čítala 1263 skupin, které byly různě přiděleny 178 identitám. Původní představa o postupu analýzy byla taková, že ze získaných dat o přidělených skupinách jednotlivým uživatelům budou vytvořeny přehledy všech pracovních pozic ve společnosti a k nim vázané skupiny, tím by vznikly tzv. business role. Vzhledem k množství skupin a faktu, že ve společnosti nebyl aktuální kompletní přehled o používaných skupinách, bylo nejprve nutné pochopit detailně organizaci a potřeby jednotlivých oddělení.

Za tímto účelem bylo potřeba zpracovat podkladová data získaná exportem skupin z Active Directory. Ta byla očištěna od duplicit a vznikl soubor všech uživatelských skupin. Data byla dále detailněji roztržena a vznikl soubor dat, který popisoval aktuální seznam skupin pro každou pracovní pozici ve společnosti.

Takto připravená data byla použita jako podklad pro schůzky s vedoucími jednotlivých oddělení, které byly pro účel této analýzy domluveny. Vedoucímu byl vždy na začátku krátce představen samotný projekt a vysvětleno jaké přínosy skýtá identity management řešení pro společnost a pro něho samotného. To vedlo k tomu, že všichni vedoucí pracovníci byli ochotnější věnovat řešení svůj čas.

Výstupem schůzky byl seznam aktuálně používaných skupin pro každou pracovní pozici spadající pod dané oddělení. Během analýzy byly také určeny skupiny, které musí být ze správy identity managementu vyloučeny a nadále spravovány ručně, případně nejsou pod správou společnosti (skupiny spravuje mateřská společnost).

3.4.2 Definice rolí, meta rolí a oprávnění

Autor na tomto místě považuje za vhodné zmínit obecný přístup IdM řešení midPoint k rolím a oprávněním.

Obecně midPoint pracuje s třemi pojmy: role, služby a organizační jednotky. Ty jsou navrženy k opakovanému používání a pro různé účely. Mají některé vlastnosti společné, ale také se mezi sebou liší. Pochopení rozdílů by mělo vést ke správnému použití. (Semančík 2016)

Role: slouží k definici schémat pro poskytování a řízení přístupu. Identitám poskytují oprávnění. Existuje více typů rolí podle použití. K řízení oprávnění midPoint používá RBAC (Role-Based Access Control) mechanismus, tedy řízení oprávnění založené na roli.

Jedná se o univerzální model řízení přístupu, zveřejněný v roce 1992. Je tvořen třemi základními pravidly (Ferraiolo a Kuhn 1992):

- **Přiřazení role:** subjekt může provést transakci pouze, pokud je přiřazen roli. Za transakci jsou považovány všechny činnosti subjektu s výjimkou přihlášení. Z toho vyplývá, že každý aktivní uživatel musí mít přiřazenu alespoň jednu aktivní roli.
- **Autorizace role:** role musí být autorizována pro subjekt. Spolu s přiřazením role tedy zajišťuje, že subjekt může získat pouze role, pro které je autorizován.
- **Autorizace transakce:** subjekt může provést transakci pouze, pokud je transakce autorizována prostřednictvím členství daného subjektu v příslušné roli, a zároveň subjekt nepodléhá omezením aplikovaným napříč uživateli, rolemi a oprávněními. To spolu s předchozími dvěma body zajišťuje, že subjekt může provádět pouze ty transakce, pro které je autorizován.

Klíčovou vlastností RBAC modelu je, že veškerý přístup je řízen prostřednictvím rolí, které tvoří prostředníka mezi uživatelem a oprávněními. Role mají přiřazena jednotlivá oprávnění a uživatelům jsou přiřazeny určité role, čímž získají i oprávnění přidělených rolí a oprávnění, která zdědí v rámci hierarchie rolí. To vede ke snížení administrativních nákladů. Další výhodou je, že v rámci společnosti jsou role relativně stabilní. Naproti tomu uživatelé a oprávnění se většinou mění velmi rychle. Dochází tedy k zjednodušení správy a kontroly řízení přístupů. Role, i když to samozřejmě není nutností ani jedinou možností, jak role použít, pak mohou vycházet typicky z jednotlivých pracovních pozic (Bertino a Takahashi 2011; Ferraiolo a Kuhn 1992).

V průběhu dalších let byl RBAC model různě rozšiřován. Evolveum midPoint používá rozšířenou verzi Advanced Hybrid RBAC. Ta k původnímu modelu RBAC (tedy, že uživateli je přiřazena určitá role a s ní i všechna z ní vycházející práva) přidává část logiky, a to možnost specifikovat výrazy v definici role, které určí, kdy a jak se role použije. Z toho vyplývá, že role se může přizpůsobit atributům uživatele nebo může být samotné přiřazení rolí parametrizováno (Semančík 2018a).

Toto rozšíření má vést k vytváření struktur s menším počtem rolí, a díky tomu se IdM řešení stává dobře ovladatelným. Často totiž při použití RBAC modelu dochází k tomu, že počet rolí začne rapidně narůstat, a poté celé řešení ztrácí svou sílu a stává se těžko spravovatelné.

K pochopení rozšíření modelu je dobré porozumět rozdílu mezi přiřazením a indukci role. Indukce se neaplikují přímo. Všechny indukce jsou aplikovány na objekty, které obsahují přiřazení, což je uživatel. Síla odlišení přiřazení a indukce se projeví zejména při použití generické synchronizace. MidPoint aplikuje RBAC mechanismus na samotné role. Proto vznikl koncept meta rolí. Meta role je role, která je aplikována jinou běžnou rolí v midPointu. Role tak obsahuje pouze přiřazení, a pokud chceme upravit konfiguraci, stačí změnit meta roli a daná změna se aplikuje na všechny ovlivněné role pomocí RBAC mechanismu. Mohou tak být tedy tvořeny role, které jsou aplikovány na jiné role nebo

organizační skupiny. To je výhodný nástroj k definování různých synchronizačních schémat pro synchronizaci rolí do skupin a oprávnění identitám velmi flexibilním způsobem. Všechny tyto konfigurace jsou jasně organizovány do několika meta rolí stále v rámci RBAC mechanismu. Meta role dále zůstávají rolemi, a tím pádem je jejich přiřazení kontrolováno, může podléhat schválení a dalším operacím (Semančík 2017).

Služby: reprezentují servery, tiskárny, notebooky a další objekty, které není možné považovat za uživatele, organizační skupinu nebo roli.

Organizační skupiny: používají se pro seskupení uživatelů nebo jiných objektů. Je možné pomocí nich vytvářet organizační stromy nebo ploché struktury a je možné používat oba tyto typy současně. Existovat může několik struktur, které je možné použít pro seskupení téměř jakéhokoliv typu objektů s různou komplexností. Organizační skupiny mohou sloužit k vytvoření aplikační nebo doménové kontroly. Dalším možným využitím je seskupení rolí, vytváření katalogu rolí (využitelný například pro uživatelskou samoobsluhu), seskupení souvisejících objektů, apod. Organizační struktury jsou tedy velmi efektivní způsob seskupování věcí, vytváření stromů a hierarchií. Na druhou stranu je to vykoupeno většími nároky na údržbu a správu, než při práci s rolemi nebo službami.

Můžeme říci, že obecně je vhodné k seskupování objektů a vytváření hierarchií používat organizační skupiny. Pro specifikaci poskytované služby je vhodné používat služby a pro povolování přístupu nebo oprávnění je vhodné využívat role.

Výhodou midPoint řešení je to, že organizační struktury a služby se mohou chovat jako role, čímž skloubí flexibilitu rolí s efektivitou organizačních skupin. Používá se k tomu tzv. indukce. Příkladem jednoho z použití je „automatické“ přiřazení rolí členům určité organizační skupiny. Stejný princip indukce platí i pro služby (Semančík 2016).

Výsledkem, analýzy skupin v Active Directory popsané v předchozí kapitole 3.4.1, bylo vyčištění Active Directory od nepoužívaných skupin a hlavně definice celkově 69 business rolí, které jsou v nasazení IdM midPoint označovány jako role. K jednotlivým business rolím byly přiděleny příslušné oprávnění definované skupinami z Active Directory, v IdM midPoint označovány opět jako role. A nakonec byla také v rámci analýzy vyčleněna samostatná specifická oprávnění, o která si bude moct žádat uživatel v samoobsluze. Příkladem takového oprávnění je barevný tisk. Všechna oprávnění jsou založena na právu allow (povoleno). Business role a oprávnění jsou propojené za použití atributu.

Organizační skupina byla použita pro reprezentaci hierarchické organizační struktury společnosti. Ta slouží k validnímu automatickému nastavení vedoucího pracovníka pro každého zaměstnance při založení nebo změně pracovní pozice či vedoucího pracovníka.

Tabulka 2 zobrazuje příklad jedné z definovaných rolí. Záhloví obsahuje název business role a obsah tabulky tvoří jednotlivá oprávnění kopírující skupiny v Active Directory.

Tabulka 2 Příklad business role (vlastní zpracování)

Call Centrum Temporary Worker	
Domain Users	CZ-AM-Fispro
CZ DL CTY All users	CZ-SD-voicemail-manazer
CZ-USER Policy	CZ-CTX Recepce
CZ-TSOFT2	CZ-Citrix-users
CZ-LEASING	CZ-ALD CZ Call Center
CZ-ZAKONY	CZ-SD-callcentrum
CZ-PRAHA	CZ-CallCenter
CZ-users	CZ-SD-voicemail-operator
CZ-CTX Desktop	CZ-VraceniVozu
CZ-XENIA	CZ-SD-ZO-administrace
CZ-CTX Zakaznicke	CZ-INFO
CZ-CTX Users	CZ-FS-Leasing-Postovnik
CZ-SD-stiznosti-operator	CZ-SAFE-Import-Sken-RWC
CZ-CustomerCare	CZ-SAFE-Modul-Import-RWC

3.4.3 Napojení Active Directory

Napojení zdrojů (systémů) pro fungování v rámci IdM obecně probíhá skrze tzv. konektor. Konektor je malý kód v jazyce Java, který komunikuje mezi IdM systémem a zdrojem. Konfigurační systémy mají podobu XML souborů a pro ně definovaných XML schémat. MidPoint při spuštění automaticky vytvoří nové konfigurační objekty pro všechny konektory, které objeví (Semančík 2018c). Příklad objektu konektoru zobrazuje Výpis 1 (z důvodu přehlednosti zkrácen).

Výpis 1 Objekt konektoru (vlastní zpracování)

```

1 <connector oid="6a31d41b-85a5-4ec4-a006-0e86a01cff68">
2   <name>ICF com.evolveum.polygon.connector.ldap.ad.AdLdapConnector v1.6.1</name>
3   <framework>http://midpoint.evolveum.com/xml/ns/public/connector/icf1</framework>
4
5   <connectorType>com.evolveum.polygon.connector.ldap.ad.AdLdapConnector</connectorType>
6   <connectorVersion>1.6.1</connectorVersion>
7   <connectorBundle>com.evolveum.polygon.connector-ldap</connectorBundle>
8   <namespace>http://midpoint.evolveum.com/xml/ns/...</namespace>
9   <schema>
10  ...
11  </schema>
12 </connector>
```

Ke zdroji se konektor jednoduše připojí přes unikátní identifikátor objektu (OID) v konfiguraci zdroje. Výpis 2 ukazuje příklad připojení (z důvodu přehlednosti zkrácen).

Výpis 2 Připojení konektoru přes OID (vlastní zpracování)

```
1 <resource>
2   <name>LDAP</name>
3   <connectorRef oid="6a31d41b-85a5-4ec4-a006-0e86a01cff68"/>
4   ...
5 </resource>
```

Konektory, které midPoint nenajde automaticky nebo byly vytvořené v naší společnosti, se přidají velmi jednoduše. Stačí nahrát JAR soubor do složky icf-connectors v domovské složce midPointu a restartovat jej.

Po úspěšném připojení potřebných konektorů je potřeba provést jejich konfiguraci pro fungování se zdroji. Obvykle jsou vyžadovány parametry síťového připojení (hostname, port, login, atd.), dále má každý konektor své vlastní vlastnosti, které je potřeba nakonfigurovat (Semančík 2018c). Výpis 3 (z důvodu přehlednosti zkrácen) ukazuje, jak konfigurační soubory mohou vypadat.

Výpis 3 Konfigurace konektoru (vlastní zpracování)

```
1 <resource oid="b4101662-7902-11e6-9f14-53e18426fe81">
2   <name>LDAP</name>
3   <connectorRef oid="6a31d41b-85a5-4ec4-a006-0e86a01cff68"/>
4     <connectorConfiguration>
5       <configurationProperties>
6         <host>10.210.1.50</host>
7         <port>636</port>
8         <connectionSecurity>ssl</connectionSecurity>
9         <baseContext>DC=automotive,DC=ald,DC=socgen</baseContext>
10        ...
11      </configurationProperties>
12    </connectorConfiguration>
13    ...
14 </resource>
```

Konektory podporované midPointem jsou založeny na dnes již nepodporovaném Identity Connector Framework (ICF), vytvořeném společností Sun Microsystems. Tento framework podporuje konektory psané technologií Java a .NET. Podporované konektory midPoint sdružuje pod projektem zvaným Polygon a jsou dostupné přes platformu GitHub (Procházka 2018).

3.4.4 Práce s uživatelskými účty

Po úspěšném navázání komunikace mezi IdM a AD je pro práci s uživatelskými účty potřeba vybrat atributy z AD, se kterými bude pracovat IdM. K tomu slouží na straně IdM formulář s předdefinovanými položkami. Samozřejmě je možné vytvořit i své vlastní položky a k těm přiřadit příslušné atributy z AD. Položky formuláře se skládají z prvků textové pole nebo výběrový seznam. Definici vztahů mezi prvky IdM formuláře a AD atributů zajišťují opět XML soubory. Každému formulářovému prvku z IdM je možné přiřadit jeden atribut z AD, nebo formulářový prvek použít jako číselník atributů z AD, a tím pádem na základě jedné položky v IdM zajistit vyplnění více atributů v AD.

Příklad zajímavého nastavení, které bylo využito při konfiguraci – pro nový účet je v IdM jedna z povinných položek lokalita. Jedná se o výběrový seznam se sedmi položkami pojmenovanými podle města, kde se lokalita nachází (např. ALD CZ Praha). Na lokalitu je vázáno 9 atributů AD pro každou lokalitu: physicalDeliveryOfficeName, wWWHomePage, streetAddress, l, postalCode, co, c, countryCode, company.

V případě konfliktu stejných jmen při vzniku identit bylo rozhodnuto, že k nové identitě je vždy přidáno následující pořadové číslo (např. Gut, Gut1, Gut2, atd.).

Po napojení AD a korektnímu nastavení požadovaných atributů identity došlo na závěr k připojení nového konektoru pro komunikaci s Exchange serverem, kdy IdM po založení identity v AD spustí na Exchange serveru PowerShell skript, který mailbox dle definovaných pravidel automaticky vytvoří. Příklad takového skriptu:

```
Enable-Mailbox -Identity  
'automotive.ald.socgen/Delegated/CZ/Accounts/Users/IDMtest/ZLUTOUCKY Konik' -Alias  
'Konik.ZLUTOUCKY' -Database 'CZ-PRAHA01'
```

Mazání uživatelů je konfigurováno tak, že pokud v IdM je uživatel označen za zakázaného (disable), tak v AD dojde také k jeho zakázání a identitě jsou odebrány veškeré skupiny. Výhodou tohoto řešení je, že v případě, kdy dojde k obnovení identity v IdM, dojde také k plnému obnovení identity i s dříve přidělenými skupinami v AD.

IdM midPoint podporuje tři režimy práce s atributy:

- Silné – co je v IdM se vždy přepíše do AD, bez ohledu na aktuální nastavení v AD.
- Normální – dokud se v IdM nezmění, zůstává, co je nastaveno v AD.
- Slabý – pokud v AD není žádná hodnota, nastaví se podle IdM. Pokud je, zůstane nezměněna.

Tyto režimy umožňují nastavit, který ze systémů bude v rozhodování o změnách hodnot atributů autoritativní. Cílem automatizovaných IdM systémů je dostat se do stavu konfigurace, kdy může být režim Silné využíván co nejvíce. Na druhou stranu, během testování nebo na začátku reálného provozu se spíše doporučuje používat slabší režimy, aby nedošlo k možné ztrátě poškození dat v AD.

3.4.5 Uživatelská samoobsluha

Uživatelská samoobsluha uživateli přináší možnost žádat o specifická oprávnění případně změnu role přes webové rozhraní. IdM řešení midPoint nabízí funkčnost samoobsluhy v uživatelsky velmi přívětivém a praktickém provedení, protože funguje stejně jako nákupní košík na e-shopu, se kterým se pravděpodobně každý uživatel alespoň někdy setkal.

Pro fungování samoobsluhy bylo potřeba definovat jaké role a oprávnění mají být pro uživatele v nabídce. Přidání role do nabídky se v IdM udělá jednoduchým nastavením přímo na požadované roli, kde se aktivuje formulářové pole Žadatelná. V ten moment se role zobrazí v nabídce uživateli.

Dále je potřeba nastavit schéma schvalování. Určit jaká identita bude moci přidělení role schválit. Ve společnosti bylo rozhodnuto, že uživatelský požadavek ze samoobsluhy vždy schvaluje nadřízený žadatele. Určení nadřízeného vychází z organizační skupiny, pro jejíž vytvoření byl použit existující organigram společnosti. Jediný konflikt, který tato konfigurace schvalování přináší, představují žádosti identit, které představují nadřízené. V tom případě totiž žádost schvaluje nadřízený sám sobě.

3.4.6 Zhodnocení nasazeného řešení

Ve společnosti ALD Automotive s.r.o. se podařilo nasadit IdM řešení Evolveo midPoint do fáze, kdy je možné spravovat identity přes IdM systém. Na základě vyplnění formulářové stránky v IdM systému dojde k vytvoření identity, kterou následně propaguje dle nastavených pravidel do AD. Jakákoli následná editace identity v IdM se propaguje do AD. Identitu je také možné zablokovat. V takovém případě identita sice v IdM i AD zůstává, ale není možné ji používat a je zbavena veškerých skupin a oprávnění, které měla. Toto řešení bylo zvoleno na rozdíl od úplného smazání z důvodu snazší obnovy identit. V případě, že by se zaměstnanec vrátil zpět do společnosti stačí účet pouze povolit v IdM, a ten bude v AD obnoven ve stejné konfiguraci jako před zablokováním i s obnoveným zařazením do příslušných skupin a oprávnění. Uživatel si může sám žádat o přidělení jednotlivých oprávnění a rolí v samoobslužném portálu. Schvalovatelem přidělení je nadřízený žadatele.

Systém obsahuje základní auditorské informace. Kdy a na základě jakého požadavku došlo k založení, editaci či smazání identity. Kdo, kdy a komu přidělil oprávnění či roli. Co, kdy a kým bylo identitě upraveno.

Samotnému nasazení předcházela analýza skupin a identit popsaná v kapitole 3.4.1. Došlo k vytvoření vzorových business rolí pro každou pracovní pozici a určení speciálních oprávnění, o které mohou uživatelé žádat v samoobsluze. Do této doby, nebyl ve společnosti komplexní přehled o používaných skupinách, a proto byla tato fáze časově náročná. Bylo nutné revidovat všechny skupiny a definovat základní rozsah pro jednotlivé pracovní pozice. Tuto analýzu bylo nutné provést a komunikovat s vedoucími jednotlivých oddělení. Dále bylo samozřejmě nutné připravit serverové prostředí pro instalaci IdM systému.

V této etapě nasazení nebyly řešeny možnosti dalšího rozvoje IdM řešení. Tím je podpora automatizace specifických identit. Příkladem mohou být externí zaměstnavatelé a část

Dodavatelů, kterým se vytváří účty dle jiné logiky. Převážně s těmito identitami je spojeno i časové hledisko platnosti identity, které v této fázi nebylo plně dořešeno. Dále je možné funkčnosti IdM řešení rozšiřovat na další systémy společnosti. Momentálně systém obsahuje pouze základní auditorské informace. Vhodným rozšířením by bylo zavedení inventury rolí, kdy by byl nadřízenému zasílán pravidelně report o přístupových oprávněních jeho podřízených. Nebyla také řešena plná automatizace správy účtu, které je možné docílit napojením IdM na tiketovací systém společnosti. Dále je možné rozšířit žadatelné role i o role, které se vážou k jednotlivým aplikacím a kde by byl schvalovatelem vlastník aplikace nebo zodpovědná osoba, protože v tomto případě má lepší přehled o tom, co uživatel potřebuje, než jeho nadřízený.

3.5 Doporučení pro implementaci

Tato podkapitola shrnuje jednotlivé kroky procesu implementace IdM řešení Evolveum midPoint, spolu s autorovými poznatky a zkušenostmi získanými během této práce, zahrnující také chyby a možné překážky, do produkčního prostředí společnosti tak, aby je bylo možné použít při implementaci libovolného nástroje identity managementu.

Analýza současného stavu

Důležitý vstupní bod celého projektu, který vede k zamyšlení, zda je IdM řešení pro společnost potřebné a vhodné, případně v jaké míře. Ne vždy je rozhodující počet identit. Je potřeba vzít v úvahu i typy identit, které společnost používá (délka životnosti, fluktuace zaměstnanců, množství pracovišť, atd.), množství systémů, způsoby autentizace, míru zabezpečení, ale také i spokojenost zaměstnanců s aktuálním stavem.

Definice požadavků

Z výsledků analýzy současného stavu vyplynou potřeby společnosti. Ty je potřeba promítnout do definice požadavků na řešení. Při nasazení IdM řešení je vhodné zvolit postupný proces a implementaci rozdělit na jednotlivé etapy. Začít od základních funkcionalit, a poté řešení v dalších etapách rozvíjet a rozšiřovat. Často se jedná o velmi výhodný postup, díky kterému může IdM řešení vhodně růst spolu se společností.

Oslovte více dodavatelů a zkonzultujte s nimi Vaše požadavky. Pravděpodobně získáte větší povědomí o tom, co je opravdu proveditelné a co ne. Poté své požadavky revidujte, případně upravte a předejte možným dodavatelům.

Výběr řešení

Vhodný nástroj musí splňovat požadavky definované v předchozím kroku. Jistě je potřeba přihlídnout také k cenové politice nástroje i dodavatele a dostupnosti technické podpory (mnoho řešení nemá podporu v Čechách). V některých společnostech může být důležité nezapomenout na ověření dostupnosti řešení pro používané distribuce serverových operačních systémů.

Zvolte vhodnou formu spolupráce s dodavatelem. Na trhu existují jak open source, tak i proprietární nástroje. K oběma variantám jsou poskytovány i implementační služby v různém rozsahu a formě. Dejte si pozor, jak je nastavena cenová politika v otázce jednotlivých konektorů (často se jedná o volně dostupné konektory, za jejichž snadné připojení si dodavatel účtuje podstatně velké sumy).

Analýza skupin a identit

Bod, na který často upozorňují i sami dodavatelé a lze jej označit za základ úspěchu či neúspěchu implementace. Společnosti často nemají přehled o aktuálním stavu skupin a identit, není vytvořené jednotné workflow průběhu života identity, a pokud je, tak často není dodržováno.

Na začátku analýzy je potřeba rozmyslet způsob, jakým budete ke skupinám přistupovat. Cesta, která byla vybrána při implementaci, zahrnovala vytvoření business rolí podle pracovní pozice. Je velmi pravděpodobné, že pro jednotlivé pracovní pozice nebudete ihned schopni určit všechny potřebné a aktuálně používané skupiny. Připravte se tedy, že v tomto bodě bude potřeba projekt představit širšímu vedení společnosti a požadovat od nich aktivní spoluúčast na řešení. Nezapomeňte, že pro vedoucího pracovníka bude fungování IdM řešení pravděpodobně velmi abstraktní. On chce, aby jeho nový zaměstnanec měl vytvořené nebo blokové účty s jeho co nejmenším úsilím, kdykoli je to potřeba, a aby vše fungovalo bez problémů a průtahů. Zdůrazněte benefity IdM řešení v těchto aspektech. Pravděpodobně poté budou spolupráci s Vámi vedoucí otevřenější.

Během zpracování také můžete narazit na různá specifika společnosti, se kterými bude při nasazení IdM řešení potřeba počítat. Například ve společnosti, kde implementace probíhala, se jednalo o skupiny, které nejsou pod správou společnosti (spravuje mateřská společnost) a skupiny, které z provozních důvodů neměli být IdM řešením spravovány. Ty bylo potřeba vyloučit ze správy IdM a nadále je spravovat ručně.

Tento bod je časově i kapacitně náročný. S analýzou je mnohdy ochotný pomoci i dodavatel řešení, v tom případě si ale dejte pozor na cenové podmínky takové analýzy.

Definice rolí a oprávnění

Zde záleží na přístupu zvoleného IdM řešení k rolím a oprávněním. Od toho se poté odvíjí možnosti konfigurace. Obecně lze tento bod považovat za finální výstup předchozího bodu. V tuto chvíli byste již měli mít skupiny očištěny o ty, které se nepoužívají a zbylé roztríděné podle zvolené logiky.

Pokud řešení počítá i s uživatelskou samoobsluhou, zde je vhodné, zamyslet se nad oprávněními nebo rolemi, které budou uživatelům tímto způsobem nabídnuty.

Konfigurace IdM systému

Konfigurace začíná přípravou vhodného serverového prostředí. Výkonové parametry záleží na požadavcích nástroje.

Po zprovoznění instalace je potřeba provést základní systémové nastavení, a poté připojit a nakonfigurovat jednotlivé konektory. Pro běžné služby je k dispozici většinou více řešení konektorů, a to v open source i proprietárních formě. Zde již hodně záleží na zvoleném IdM nástroji i dodavateli (pokud neprobíhá nasazení vlastními silami).

Podstatnou část této fáze zabere správná konfigurace jednotlivých konektorů. IdM řešení jsou z velké části opravdu spíše pouze nástrojem, než hotovým řešením, které se nainstaluje a funguje u každého zákazníka stejně nebo podobně. Na druhou stranu to přináší možnost velké míry upravitelnosti pro potřeby společnosti. To je také důvod proč se o IdM řešení říká, že neexistují dvě stejná řešení a vždy se jedná o unikátní řešení pro společnost, které je prakticky nepřenositelné pro další nasazení.

Konfiguraci mohou prodloužit nejasnosti v napojovaných systémech. Například v AD existuje atribut Country, který je závislý na vyplnění dalších tří atributů (c, co, countryCode), což při běžné práci v dialogovém okně AD vůbec nevíte. Často jsou také atributy oproti dialogovému zobrazení pojmenovány úplně jinak.

Pokud je společnost součástí korporace, je možné, že některé systémy používá více organizací a podléhají centrálním pravidlům. Společnost si je tak nebude moct upravit pro své potřeby a pro potřeby IdM řešení. Poté přichází na řadu snaha IdM přizpůsobit co nejvíce možnostech vycházejících z centrálních nařízení korporace.

Pokud je potřeba vyvinout pro napojovaný systém nový vlastní konektor, přichází na řadu diskuze o tom, jak bude probíhat výměna dat mezi IdM a zdrojovým systémem. V některých případech je nutná úprava zdroje pro možnou komunikaci s IdM.

Platí zde, že to co vypadá jednoduše v prostředí IdM může být velmi složité v napojovaném prostředí a naopak. Nezapomeňte také na časovou náročnost konfigurace. Obzvlášť, pokud IdM zavádíte do již léta fungující struktury. Počítejte s tím, že během konfigurace jistě objevíte souvislosti a historická nastavení systémů, o kterých jste ani nevěděli nebo které není možné upravit. Poté je potřeba vymýšlet, jak přizpůsobit IdM řešení a to i v případech, kdy se jedná o sebemenší detaily.

Testování

Protože IdM zasahuje přímo do ostatních systémů je před plným produkčním spuštěním zásadní důkladné testování konfigurace a práce IdM. Vhodné je provést vždy před nasazením IdM na zdrojový systém jeho zálohu, pokud je to možné. Pokud ne, je potřeba postupovat o to opatrněji.

V systémech, kde je to možné se osvědčilo testovat nejdříve na oddělených identitách od produkčního prostředí. Po odchycení a vyřešení chyb přejít k testování na vybraném vzorku, ideálně méně důležitých identit v produkčním prostředí a následně pokud probíhá vše korektně spustit testovací provoz na všech identitách produkčního prostředí.

Vyhodnocení

Pokud je během testování konfigurace vyhodnocena jako nevyhovující je potřeba se vrátit k předchozímu kroku konfigurace, v některých případech bude možná nutné vrátit se ještě k definici rolí a identit. Pokud je konfigurace vyhodnocena jako vyhovující, je možné přejít do reálného provozu.

Reálný provoz

Po uznání konfigurace jako vyhovující je potřeba IdM řešení dále rozvíjet spolu s růstem a změnami organizace, spravovaných systémů a nových požadavků. Za tímto účelem je vhodné stanovit časovou periodu, po které dojde vždy k revizi řešení. Počítejte, že do stavu reálného provozu se nasazení dostane minimálně v řádech měsíců.

Revize řešení

U IdM řešení jsou předpoklady pro neustálý rozvoj a změny, proto, aby bylo řešení opravu přínosem, je vhodné provádět po určité časové periodě jeho revizi. Pokud je stávající konfigurace vyhovující, probíhá stálá pasivní údržba a rozvoj s prostředím společnosti. V případě, že již vyhovující není, případně je nutné rozšíření o další systémy je vhodné vrátit se k libovolnému předešlému kroku. V některých případech až k definici rolí a oprávnění.

Závěr

Bakalářská práce se zabývá problematikou identity managementu. První kapitola uvádí čtenáře do dané problematiky, vymezuje základní pojmy a představuje co IdM řešení přináší a pro koho jsou vhodná. Druhá kapitola popisuje základní funkce a vlastnosti IdM řešení. Detailněji představuje základní pojmy, se kterými se v této problematice pracuje a představuje možnosti využití.

Třetí kapitola se zabývá praktickou implementací vybraného IdM řešení do produkčního prostředí společnosti ALD Automotive s.r.o. tak, aby pokryla stanovené požadavky, a která bude dále rozvíjena. Nejedná se o instalační dokumentaci, naopak o popsání celého průběhu a přístupu k implementaci, který je využitelný společnostmi i při výběru a implementaci IdM řešení do vlastního prostředí.

Implementace zahrnovala autorem provedenou vstupní analýzu, která obecně popisovala práci s identitami v dané společnosti. V řešitelském týmu, kterého byl autor členem, poté došlo k definování požadavků na poptávku IdM řešení a dodavatele se kterým bude implementace prováděna. Autor následně vybral a oslovil dodavatele splňující zvolená kritéria a vedl s nimi úvodní komunikaci. Výstupy z úvodních schůzek prezentoval vedení IT a zbytku řešitelskému týmu. Následně byly vybrány tři společnosti do finálního výběrového řízení. Před jeho vyhodnocením proběhla detailnější schůzka s oslovenými dodavateli, během kterých byly vyjasněny požadavky a možnosti řešení. Ve výběrovém řízení byl vybrán open source nástroj Evolveum midPoint a dodavatelská společnost GAPP System, spol. s.r.o.

Implementace byla zahájena autorovou analýzou identit a skupin, která spočívala v očištění vstupních dat a rozřídění skupin do výsledných business rolí, které kopírují pracovní pozice. V této fázi bylo nutné provést konzultace s jednotlivými vedoucími pracovníky oddělení. Dále pak definovat skupiny pro žadatelná oprávnění v uživatelské samoobsluze. Spolu s dodavatelem poté došlo k samotnému nasazení a konfiguraci nástroje Evolveum midPoint, během níž bylo nutné definovat, upravovat a konfigurovat atributy napojovaného AD a Exchange serveru s prostřením IdM. Průběžně probíhalo testování nasazované konfigurace a zpětná úprava. Výsledným stavem etapy, kterou práce popisuje, je funkční IdM řešení komunikující s AD, přes které je plně možné spravovat doménové identity společnosti.

V průběhu implementace se objevili problémy, které projekt časově ohrožily. Mimo vzniklé otázky přímo při implementaci i časové vyčerpání dodavatele. Přesto byl časový harmonogram v zásadě dodržen a stanovenou fází se podařilo dokončit. Implementaci je tak možné považovat za úspěšnou. Na vyhodnocení vnímání změn uživateli je ještě brzy. Jistě je ale vhodné, po několika měsících ostrého provozu analýzu uživatelské spokojenosti provést, protože i ta by měla být jedním z benefitů zavedení IdM řešení.

V budoucnu lze očekávat rozšíření hlavně o napojení IdM na požadavkový systém společnosti, čímž dojde k plné automatizaci zakládání a rušení uživatelských identit v AD, kdy

vstupním impulzem pro práci IdM bude pouze vytvořený požadavek zodpovědné osoby v požadavkovém systému. Funkčnost IdM bude dále vylepšena dořešením časového hlediska správy identit, prohloubením auditorských možností, zahrnující inventuru rolí jednotlivých identit. Dále se počítá s rozšiřováním automatizace na další systémy a s nimi spojené identity. Předpokládá se rozšíření žadatelných oprávnění v uživatelské samo-obsluze o aplikační role. Dále je možné zabývat se automatizací specifických identit, které se ve společnosti vyskytují.

Závěrečná podkapitola 3.5 obsahuje autorem sestavené doporučení pro implementaci libovolného IdM řešení, jež může být společností využito při výběru a implementaci IdM do vlastního prostředí.

Hlavní přínos práce spočívá v úspěšné implementaci IdM nástroje do prostředí reálné společnosti, nakonfigurovaný tak, aby pokryl stanovené požadavky, a který bude používán pro správu identit a dále rozvíjen, jak bylo nastíněno v předchozích odstavcích. V průběhu implementace došlo k přehodnocení cíle a bod napojení požadavkového systému byl přesunut do další fáze projektu.

Pro čtenáře je dále přínosem komplexní pohled na problematiku správy identit, spolu s obecnými doporučeními pro implementaci IdM řešení, které by mělo být platné i v rychle rozvíjejícím se oboru, kterým správa a řízení identit je.

Použitá literatura

BERTINO, Elisa a Kenji TAKAHASHI, 2011. *Identity management: concepts, technologies, and systems*. Boston: Artech House. Information security and privacy series. ISBN 978-1-60807-039-8.

CIRKVA, Lukáš, 2018. Co je to Identity Management. *BCVlog* [online]. [vid. 2019-02-19]. Dostupné z: <https://blog.bcvolutions.eu/co-je-to-identity-management/>

ELCOMSOFT, 2009. *Password Security Survey 2009* [online] [vid. 2019-04-24]. Dostupné z: <http://passwordresearch.com/stats/study125.html>

EVOLVEUM, 2018a. *evolveum-presentation.pdf* [online]. 2018. [vid. 2019-03-12]. Dostupné z: <https://evolveum.com/wp-content/uploads/2018/11/evolveum-presentation.pdf>

EVOLVEUM, 2018b. *GDPR and open source identity management (IDM) solution midPoint* [online]. [vid. 2019-03-12]. Dostupné z: <https://evolveum.com/gdpr/gdpr-midpoint/>

EVOLVEUM, 2018c. *MidPoint: open source identity management & data governance software* [online]. [vid. 2019-03-12]. Dostupné z: <https://evolveum.com/midpoint/>

FERRAILOLO, David a Richard KUHN, 1992. Role-Based Access Controls. In: *15th National Computer Security Conference (NCSC); October 13-16, 1992; Baltimore, Maryland, United States: Proceedings of the 15th National Computer Security Conference* [online]. s. 554–563 [vid. 2019-04-03]. Dostupné z: <https://csrc.nist.gov/publications/detail/conference-paper/1992/10/13/role-based-access-controls>

GAPP SYSTEM, 2014. O nás. *GAPP System* [online] [vid. 2019-03-10]. Dostupné z: <http://www.gapp.cz/o-nas>

GARTNER INC., 2019. *Identity Management – Access Management – Gartner Research* [online] [vid. 2019-02-19]. Dostupné z: <https://www.gartner.com/it-glossary/identity-and-access-management-iam/>

GAŠPAŘÍK, Petr, 2018. *Access a key distribution system – Seriál o IdM, část 4*. [online] [vid. 2019-02-25]. Dostupné z: <https://www.kybez.cz/clanky/detail?urltitle=access-a-key-distribution-system-serial-o-idm-cast-4->

GEALFOW, John, 2016. *Právo na soukromí – Iurium Wiki* [online] [vid. 2019-02-19]. Dostupné z: https://wiki.iurium.cz/w/Pr%C3%A1vo_na_soukrom%C3%AD

IDMWORKS, 2015. Authentication & Authorization. *IDMWORKS* [online]. [vid. 2019-02-26]. Dostupné z: <https://www.idmworks.com/identity-access-management/authentication-authorization/>

ISO/IEC, 2011. *Information technology – Security techniques – A framework for identity management*. 2011.

ITU-T, 2009. *NGN identity management framework* [online]. leden 2009. Geneva: ITU-T. Dostupné z: <https://www.itu.int/rec/T-REC-Y.2720-200901-I>

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. *Výkladový slovník kybernetické bezpečnosti* [online]. 2015. Dostupné z: https://cybersecurity.cz/data/slovník_v310.pdf

KREJČÍ, Jan, 2008. *Správa identity* [online] [vid. 2019-02-23]. Dostupné z: <http://www.systemonline.cz/sprava-it/sprava-identity.htm>

MOORE, Chuck, 2014. The Role of Authentication in Identity Management. *Identity Services at Penn State* [online] [vid. 2019-02-25]. Dostupné z: <http://www.identity.psu.edu/resources/documentation/current/the-role-of-authentication/>

NORSIS, 2012. *NorSIS Password Survey 2012* [online] [vid. 2019-04-24]. Dostupné z: <http://passwordresearch.com/stats/study118.html>

PASCUAL, Al, Kyle MARCHINI a Sarah MILLER, 2018. *Identity Fraud: Fraud Enters a New Era of Complexity | Javelin* [online] [vid. 2019-04-01]. Dostupné z: <https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity>

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Aleš Čeněk. ISBN 978-80-86898-38-4.

PROCHÁZKA, Peter, 2018. *Identity Connectors – midPoint – Evolveum Confluence* [online] [vid. 2019-04-05]. Dostupné z: <https://wiki.evolveum.com/display/midPoint/Identity+Connectors>

SEMANČÍK, Radovan, 2016. Roles, Services and Orgs – midPoint – Evolveum Confluence. *Roles, Services and Orgs* [online] [vid. 2019-03-22]. Dostupné z: <https://wiki.evolveum.com/display/midPoint/Roles%2C+Services+and+Orgs>

SEMANČÍK, Radovan, 2017. *Roles, Metaroles and Generic Synchronization – midPoint – Evolveum Confluence* [online] [vid. 2019-03-22]. Dostupné z: <https://wiki.evolveum.com/display/midPoint/Roles%2C+Metaroles+and+Generic+Syn+chronization>

SEMANČÍK, Radovan, 2018a. *Advanced Hybrid RBAC – midPoint – Evolveum Confluence* [online] [vid. 2019-04-04]. Dostupné z: <https://wiki.evolveum.com/display/midPoint/Advanced+Hybrid+RBAC>

SEMANČÍK, Radovan, 2018b. *midPoint History – midPoint – Evolveum Confluence* [online] [vid. 2019-03-12]. Dostupné z: <https://wiki.evolveum.com/display/midPoint/midPoint+History#midPointHistory-ProjectStart>

SEMANČÍK, Radovan, 2018c. *Practical Identity Management with midPoint* [online]. 2018. [vid. 2019-04-05]. Dostupné z: <https://evolveum.com/wp-content/uploads/2018/04/practical-idm-with-midpoint-1.1.pdf>

SEMANČÍK, Radovan, Ivan NORIS a Stanislav GRÜNFELD, 2015. *Cesta k efektivnímu identity managementu (6. díl)* [online] [vid. 2019-03-04]. Dostupné z: <http://www.systemonline.cz/it-security/cesta-k-efektivnimu-idm-pokrocile-technologie.htm>

SHANKAR, Vijay, 2016. *Does Password Reset on a Service Desk cost us money ? Yes it does. Wake up!!!* [online] [vid. 2019-03-05]. Dostupné z: <https://www.linkedin.com/pulse/does-password-reset-service-desk-cost-us-money-yes-wake-vijay-shankar>

SIKORA, Tomáš, 2003. *Identity Management* [online] [vid. 2019-02-19]. Dostupné z: <https://www.systemonline.cz/clanky/identity-management.htm>

STAUDEK, Jan, 2006. *Správa identit, Identity Management, IDM* [online]. 2006. Dostupné z: https://www.fi.muni.cz/usr/staudek/vyuka/security/case_studies/09_IDM.ps.pdf

TECHOPEDIA, 2019. What is an Identity Life Cycle? – Definition from Techopedia. *Techopedia.com* [online] [vid. 2019-02-19]. Dostupné z: <https://www.techopedia.com/definition/32205/identity-life-cycle>

VOHNOUTOVÁ, Marta, 2008. *Identity a access management* [online] [vid. 2019-02-23]. Dostupné z: <http://www.systemonline.cz/sprava-it/identity-a-access-management-1.htm>

WALKER, Alfred J., 2003. *Moderní personální management: nejnovější trendy a technologie*. Praha: Grada Publishing a.s. ISBN 978-80-247-0449-4.

WATERS, James A. Martin and John K., 2018. What is IAM? Identity and access management explained. *CSO Online* [online] [vid. 2019-02-19]. Dostupné z: <https://www.csoonline.com/article/2120384/identity-management/what-is-iam-identity-and-access-management-explained.html>