IDENTITY MANAGEMENT NA PRAŽSKÉM MAGISTRÁTU

Řízení uživatelských identit, oprávnění a rolí neboli Identity Management (dále jen IdM) dnes patří mezi základní stavební kameny komplexního bezpečného IT prostředí středních a velkých organizací. Zjednodušeně řečeno se jedná o centralizovanou správu uživatelů v systémech používaných danou organizací, ve skutečnosti jde ale o mnohem více. IdM přináší zvýšení bezpečnosti z pohledu přístupu uživatelů k informačním zdrojům, zrychluje procesy spojené s přidělováním či odebíráním oprávnění, zjednodušuje správu jinak neuvěřitelně velkého množství rolí a odpovídá na mnohé otázky či výtky auditorů.

Složitost zavedení systému IdM závisí na počtu připojovaných systémů a také na tom, co všechno se od takového systému čeká. I v této oblasti může být zaveden systém velmi jednoduše jen se základním setem funkcí, například jen s propagací uživatelských oprávnění do koncových systémů. Pokud se ale k IdM problematice přistoupí komplexně, může vzniknout systém, který pomůže mnohem více – zautomatizuje proces kontroly oprávnění na koncových systémech, zavede systém tzv. business rolí pro jejich jednoduché navázání na organizační strukturu, automaticky kontroluje přidělování konfliktních rolí, obsahuje pravidla pro mnoho automatizovaných operací či obsahuje uživatelskou samoobsluhu, ve které si uživatelé mohou měnit hesla, žádat o nové role, kontrolovat na ně směřované úkoly, nebo třeba sledovat, kde se ve schvalovacím workflow nachází jejich požadavek.

Pojďme se podívat, jak k této problematice přistoupili na Magistrátu hl. m. Prahy (dále jen MHMP), kde si jako nástroj pro správu identit vybrali v rámci VZ open-source produkt IdM midPoint a implementátora AMI Praha a.s.

MHMP jako instituce řídící jeden ze samosprávních celků v ČR má z pohledu IT celkem cca 2 500 fyzických uživatelů a přes 70 různých aplikací a systémů. Podobně jako jiné velké instituce si během své existence v informačním věku vybudoval svébytné procesy správy uživatelů a přidělování práv. Ty byly v řadě ohledů poměrně efektivní, ale zároveň složitě přenositelné do automatizovaného prostředí. Zároveň zde existovaly procesy poplatné prostředí bez IdM typu „Přidělte prosím panu XY stejná práva, jako má paní YZ“, což je z pohledu zajištění aktuálnosti a udržitelnosti v tak velké instituci a počtu aplikací velmi náročné.

Cíle a očekávání

MHMP proto k novému projektu přistoupil důsledně a dal si za cíl vytvořit systém, který nedovolí operace s identitami – vznik, změny, zánik, přidělování a odebírání rolí – mimo procesy kontrolované ze strany IdM midPoint. Nezbytným požadavkem byla zpětná auditovatelnost těchto operací. Cílem bylo mj. postavit systém, který zaručí MHMP soulad se zákonem o kybernetické bezpečnosti a platnou legislativou v oblasti ochrany osobních údajů (GDPR) v jejich patřičných kapitolách.
Cílem a de facto očekáváním bylo tedy zajištění řízení životního cyklu uživatelů a řízení přístupů do koncových systémů MHMP (myšleno agend úřadu), získání kontroly nad veškerými změnami na úrovni organizačního zařazení uživatelů a zajištění automatického promítnutí změn do koncových systémů.

Přínosy

Implementací IdM v požadovaném rozsahu se tak dosáhlo očekávaných přínosů projektu:

- zrychlení přidělování přístupů do koncových systémů;
- odstranění chybovosti při přidělování oprávnění (odstraněním lidského faktoru);
- zvýšení bezpečnosti a řiditelnosti na základě centralizace správy oprávnění;
- podpora vynutitelnosti bezpečnostních politik v oblasti komplexnosti hesel;
- automatizace vzniku podkladů pro pravidelné audity (kdo, kdy a na základě čeho má přístup do koncových systémů a pod jakým oprávněním);

- řízení rolí s konfliktními oprávněními (SoD);
- zjednodušení řízení oprávnění prostřednictvím tvorby systému business rolí (v budoucnu bude možné využít funkcionalitu certifikačních kampaní pro pravidelné ověřování jejich aktuálnosti);
- automatizace vybraných operací prostřednictvím pravidel;
- logování veškerých operací a podpora pro audity.

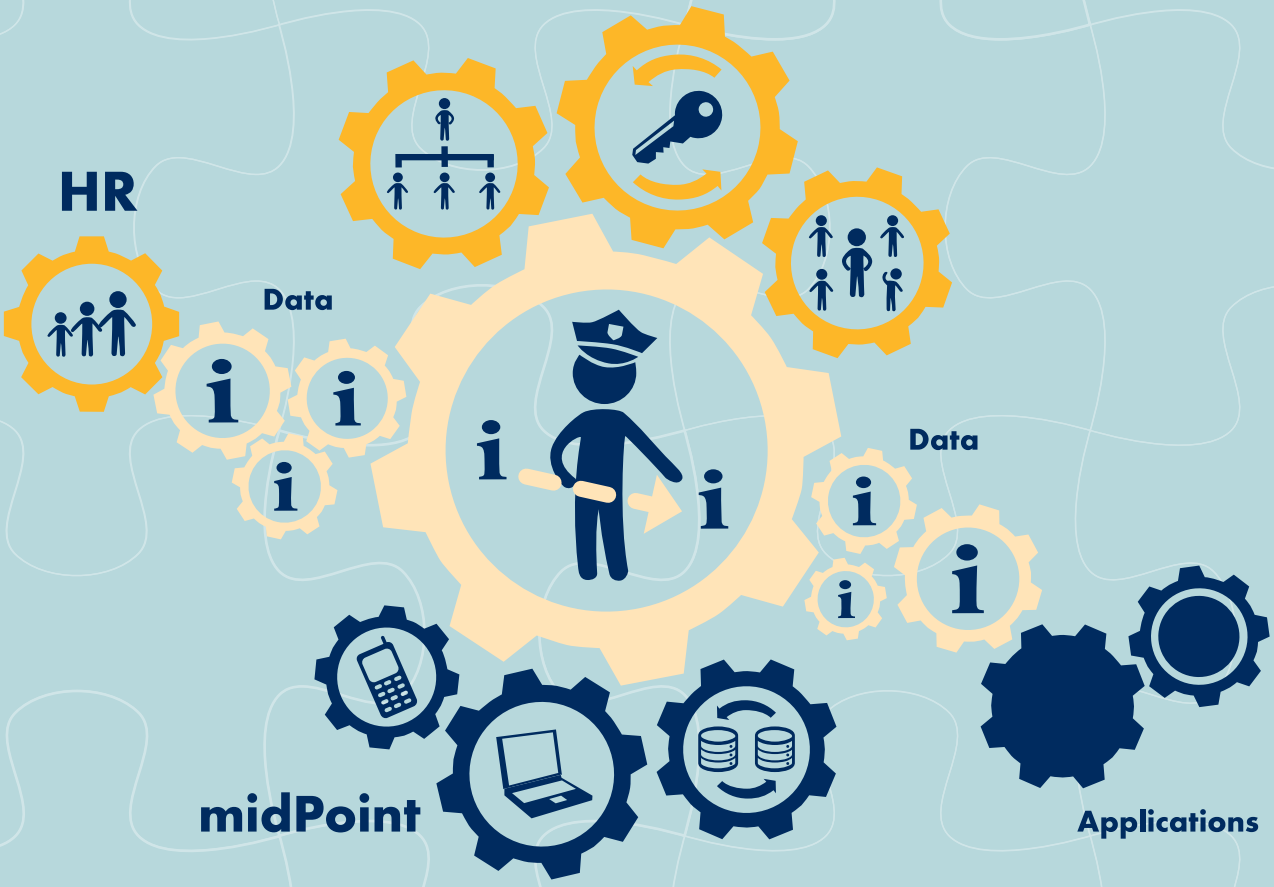
Celkově se tedy zavedením IdM urychlily a zjednodušily procesy spojené s přidělováním uživatelských oprávnění, zautomatizovala se aktualizace oprávnění v koncových systémech na základě změn v HR agendě a zvýšila se bezpečnost přístupu uživatelů do koncových systémů a přehlednost o nich.

Analýza a návrh

Projekty zavádění IdM vyžadují komplexní analýzu existujících a požadovaných procesů a funkcionalit a nejinak tomu bylo v případě MHMP. Hlavními úkoly analytické části projektu bylo:

- zmapovat dosavadní obecné procesy správy identit a oprávnění;
- identifikovat, jaké aplikace a systémy MHMP vlastně identity využívají;
- podrobně analyzovat správu uživatelů, rolí a případně organizační struktury v systémech a aplikacích, jejichž napojení bylo požadováno v zadávací dokumentaci.

Náš tým organizoval analytické schůzky s účastníky napříč celým úřadem – se zástupci interní správy aplikací a infrastruktury, bezpečnosti, personálního oddělení a v neposlední řadě se zástupci dodavatelských firem, na které MHMP řadu činností správy IT technologií přenesl.
Nemůžeme potvrdit časté tvrzení o státních a veřejných institucích, že „levá ruka neví, co dělá pravá“, byli jsme příjemně překvapeni pravidelnými informacemi z paralelně běžících projektů. To nám umožnilo využít i některé jejich výstupy a celkově tak naše úsilí zefektivnit.
Pro všechny systémy má MHMP stanoveny dva druhy garantů – věcné, zodpovědné za to, aby systém správně plnil svou „business“ úlohu v instituci, a technické, zodpovědné za každodenní provoz. Při analýze konkrétních systémů jsme pracovali s informacemi od obou druhů garantů a v další fázi i přímo od dodavatelů aplikací.



Není překvapením, že vesměs všichni pracovníci MHMP, se kterými jsme potřebovali hovořit, jsou velmi časově vytížení. První velkou výzvou analytické části tak bylo dostat co nejdříve ty správné lidi společně do zasedací místnosti. A mohlo se začít.

Naším výstupem byl návrh implementace IdM, který počítal s personálním systémem jako autoritativním zdrojem identit. Existuje základní sada přístupů, které jsou pak automaticky přidělovány všem novým zaměstnancům (Active Directory, agendové systémy). O přístup do dalších aplikací žádají pro své podřízené vedoucí. Výhodou proti dosavadnímu stavu je, že po schválení IdM přístup automaticky v aplikaci založí přes integrační rozhraní a odpadá tak manuální zásah administrátora, který je tak o vzniku přístupu již pouze notifikován.

Důležitou součástí návrhu je integrace na interní Service Desk, jejímž cílem bylo zachovat jednotné kontaktní místo pro koncové uživatele. Pokud tedy chce např. vedoucí požádat o přístup, jde nejdříve do Service Desku, odkud je v určitém kroku automaticky přesměrován do IdM, kde vybere konkrétní systém a roli. Po potvrzení je v IdM spuštěn schvalovací proces, který je plně integrován se schvalováním v Service Desku. Své položky ke schválení uživatelé najdou na stále stejném místě jako dosud, nejsou nuceni chodit do dalšího systému.

Koncepce IdM MHMP počítá i s propojením s jednotlivými městskými částmi a městskými organizacemi, mimo jiné za účelem správy uživatelů pro systémy, které MHMP pro některé MČ a MO provozuje.

Realizace

Nejsnazší variantou propojení IdM s koncovým systémem je, pokud řízený systém používá jako zdroj uživatelů Active Directory nebo některý adresářový server dostupný přes protokol LDAP. V ostatních případech je třeba vybudovat integrační rozhraní pomocí web services nebo přímého propojení s databází.

Zajištění rozhraní na straně řízených systémů je největším rizikem pro harmonogram celého projektu. Narazili jsme na systémy, které rozhraní pro správu uživatelů měly již hotové, ale také na případy, kdy bylo potřeba rozhraní vytvořit či upravit jejich dodavateli, tedy v režimu MHMP zajistit součinnost těchto dodavatelů.

Po samotné realizaci, kterou provedl náš zkušený tým dle osvědčené projektové metodiky, následovala fáze společného testování a tedy opětovné shánění vytížených projektových kolegů. Velmi se nám osvědčilo mít v jedné místnosti zástupce všech rolí, které se procesů správy uživatelů účastní. Omezili jsme tak případná nedorozumění při vzdálené komunikaci.

Nasazování do provozu

Na MHMP byly manuální procesy správy identit zaběhlé již velmi dlouho, a změna proto nebyla jednoduchá. Brzy jsme pochopili, proč nám naši partneři na straně klienta zdůrazňují nutnost častých návštěv u správných lidí a interního marketingu obecně.

Identity management si nelze představit bez jasně daných postupů. Součástí projektu proto byly návrhy na změny interních metodik, nastavení nových zodpovědných osob a procesů a samozřejmě obvyklé druhy dokumentace, plány pro zálohování a disaster recovery a uživatelské příručky pro zúčastněné role.

Současný stav a další kroky

V současné době IdM na MHMP zajišťuje přenos identit z personálního systému do Active Directory a řízení uživatelů a přístupů (rolí) v několika základních systémech, včetně aplikace pro správu přístupových karet.

Implementační část projektu dále pokračuje a v roce 2019 bude k IdM připojeno celkem cca 20 systémů. Dlouhodobým cílem MHMP je pomocí IdM řídit identity ve všech aplikacích. Jejich integrace však není podmínkou dosažení hlavního cíle, a to řízení vzniku všech identit a přidělování jejich práv přes IdM. Systém již nyní spravuje všechny interní i externí uživatele a obsahuje role i pro aplikace, které nebudou napojené online. IdM midPoint tak umožňuje evidovat žádosti o přístupy i skutečně přidělené role pro všechny aplikace MHMP.

Projekt nasazení Identity Managementu na MHMP byl a je velkou zkušeností pro týmy na straně zákazníka i dodavatele. Spolupráci nám nyní usnadňuje především to, že jsou za společnou prací vidět konkrétní a hmatatelné výsledky s jasnou přidanou hodnotou.

Petr Urban
obchodní ředitel
AMI Praha, a. s.