Případová studie nasazení Identity Management (IDM)

Dostupné IDM řešení – bezpečnost pro každého

Zaměstnanci přicházejí, odcházejí a je nutné se o všechny postarat. Nejen aby měli své pracovní místo, ale také aby měli správné přístupy ke všem potřebným informačním systémů (IS) a také aby toto právo ztratili při odchodu ze společnosti. Proto je tady Identity management, a to nejen pro velké firmy, ale i pro malé a střední podniky.

PŘÍPADOVÁ STUDIE

Vlastnosti IDM

IDM je ryché dostupné, flexibilní a cenově přijatelné řešení, které odstraní řadu problémů v podnicích všech velikostí. Proč tedy nevyužívat i v menších společnostech technologické vymoženosti, jež si až dosud mohly dovolit jen velké korporace?

Je to tady. Nový zaměstnanec právě vkročil do budovy. Co s ním?
Aby mohl řádně pracovat, místní IT oddělení mu musí zajistit všechny potřebné přístupy do informačních systémů. Takové úkony zpravidla řeší interní předpis, typicky jde o časově náročný systém žádostí a schvalovacích procesů, kde na konci je správce informačního systému, který zajistí potřebná nastavení.

Podobné problémy, ovšem opačného rázu, řeší společnosti také v případě, že je zaměstnanci opouštějí. S jejich odchodem se navíc pojí nezanedbatelné bezpečnostní riziko. O odchodu se totiž často nedozví kompetentní osoby, které by měly příslušná oprávnění zase odebrat či ještě lépe zrušit. Riziková je i změna pozice zaměstnance, kdy často dochází ke kumulaci přístupů, protože pracovníkovi jsou přidělena nová oprávnění, ovšem původně přidělená oprávnění mu zůstávají.

Základním ochranným prvkem před podobnými problémy jsou bezpečnostní audity, kterými by měly společnosti pravidelně procházet. Část auditu by se totiž měla věnovat i správě uživatelů informačních systémů. Typický dotaz auditora zní: „Kdo a do jakých informačních systémů má povolen přístup a kdo mu jej schválil?“. Vypracování a obhájení příslušných zpráv je ovšem často „noční můrou“ pro zodpovědné manažery IT oddělení, nehledě na to, že ze závěrů auditu se firma nemusí poučit.

Kouzlo IDM

Správa identit (Identity Management – IDM) představuje informační systém, který se stará o životní cyklus identity každého uživatele, a zajišťuje tak efektivní správu jeho přístupových oprávnění. IDM je napojen na personální systém, z něhož získává informace o všech změnách v údajích o zaměstnancích (změna pozice, příjmení, nástup zaměstnance, výpověď...). Na druhé straně je IDM integrován s jednotlivými informačními systémy a automaticky spravuje uživatele IS na základě pravidel definovaných v IDM.

POSKYTNUTÉ SLUŽBY

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

Kdo nabízí IDM

Nyní je na trhu řada IDM řešení, a to jak na bázi komerčních produktů od softwarových společností Oracle, Microsoft, IBM, Novell či CA, tak i na bázi opensource řešení, jakými jsou například OpenIDM, Apache Syncope, midPoint nebo OpenIAM.

Správa identit

Každá změna u zaměstnance vyžaduje změny v nastavení uživatelských údajů v informačních systémech firmy. Specializovaný software zaručuje efektivní zvládnutí IDM agendy, kam patří zejména:

- automatická propagace změn do uživatelských účtů v IS,
- zajištění souladu v uživatelských účtech napříč IS,
- evidence všech změn a provedených akcí (audit),
- formalizace a automatizace IDM procesů,
- centrální evidence všech uživatelských účtů v IS,
- samoobslužný systém pro základní IDM úkony (změna hesla, žádost/schválení přístupových oprávnění).

Vedle automatických akcí IDM nabízí možnost přidělování přístupů na základě schválených žádostí. Schvalovací proces aktivuje založení žádosti a jednotliví schvalovatelé se odvozují z organizační struktury podniku.

IDM představuje centrální jednotnou evidenci o všech přístupových oprávnění napříč všemi informačními systémy podniku. Pro zajištění souladu informací v IDM a v integrovaných IS je nutné zpětně synchronizovat uživatelská oprávnění. Proces se nazývá „rekonciliace" a díky němu je možné detekovat neautorizované modifikace uživatelských oprávnění, které se uskutečnily mimo IDM řešení.

Díky procesu „rekonciliace" jsou veškeré aplikační účty propojeny s konkrétními uživateli, tudíž jejich veškeré aktivity jsou rychle a jasně identifikovatelné s osobní odpovědností.

Samozřejmostí IDM je i funkce auditu, která zajišťuje evidenci a následnou dohledatelnost změn v záznamech o uživateli.

IDM dovoluje využívat patřičné podnikové role (např. referentka HR, účetní, obchodní zástupce) a abstrahovat tak od konkrétních aplikačních rolí informačních systémů (např. zapis_erp_saldo, vypis_historie_banka). Využívání jednotlivých aplikačních rolí totiž není pro odborné (ne IT) úseky intuitivní a zbytečně jim tak komplikuje pracovní výkon. Naopak využíváním srozumitelně pojmenovaných podnikových rolí – jak se děje v IDM – se dosahuje výrazného zjednodušení ve všech potřebných úkonech. Navíc podnikové role jsou účinným nástrojem, který minimalizuje kumulování oprávnění při přechodu zaměstnance na jinou pozici.

Zdaleka nejlepší na tom všem je, že nejde o technologii, která by svou robustností či cenou byla dostupná jen velkým podnikům. Dá se totiž rychle a levně postavit na libovolné platformě také pro malé a střední firmy. Řada zákazníků, a to zejména ze segmentu menších firem, má obavy z finanční náročnosti IDM řešení. Pak jsou překvapeni, když zjistí, že investice nejsou v řádech milionů ale statisíců. Řídit práva a oprávnění zaměstnanců přece musí každá firma nezávisle na tom, zdali zaměstnává sto, tisíc nebo deset tisíc pracovníků.