

IDENTITY & ROLE MANAGEMENT



Každý větší podnik dnes využívá desítky informačních systémů, ke kterým mají zaměstnanci přístup a často se do nich i několikrát denně přihlašují. Správa přístupových práv u stovek zaměstnanců a desítek informačních systémů se tak postupně stává stále složitější a těžko se kontroluje. Dochází kvůli tomu ke ztrátě efektivity, chybám a dokonce i k závažným bezpečnostním problémům, kdy mají k důvěrným datům přístup i uživatelé, kteří by jej mít neměli. Vyvarujte se těchto problémů a snižte své náklady na správu uživatelů a rolí s řešením od AMI Praha.

PŘÍNOSY PRO BYZNYS

Každé IT řešení by mělo přinést úsporu nákladů, zvýšení kvality nebo bezpečnosti anebo nové obchodní příležitosti. Co přinese podniku Identity & Role Management?

► PŘEHLEDNÁ A SNADNO OVLADATELNÁ PŘÍSTUPOVÁ PRÁVA DO VŠECH SYSTÉMŮ

Každý zaměstnanec má jedny přihlašovací údaje do všech systémů – identitu. Této identitě jsou podle pracovního zaměření přiřazeny role, což je sada přístupů a oprávnění do určitých informačních systémů podniku. Díky tomu je velmi jednoduché zaměstnanci nebo celé skupině zaměstnanců udělit přístup do nového systému, případně nastavit automatické akce při odchodu zaměstnance – na nikoho a nic se tak nezapomene. Vše je správně zdokumentované a lehce dohledatelné pro interní i externí auditory. Auditóři najdou i informace o tom, kdo přidělení přístupu nebo oprávnění schválil!

REFERENCE

Identity Management jsme úspěšně implementovali např. ve společnostech CCS a ČEZ. Ve společnosti ČEZ se jednalo o největší nasazení Sun Identity Manageru ve střední Evropě, kde se pomocí systému Identity Management řídí přes 100 informačních systémů různých druhů, desetitisíce uživatelských účtů a statisíce rolí.

► LEPŠÍ ZABEZPEČENÍ

Centralizace správy uživatelských účtů a oprávnění zaručuje, že nikomu nezůstane účet v žádném systému, když už ho nepotřebuje pro svou práci, nebo když už u vás nepracuje. Systémy pro Identity & Role Management dokonce díky speciální logice hlídají, jestli někde nejsou zapomenuté uživatelské účty, které již nejsou potřeba a mohou znamenat potenciální bezpečnostní problém, nebo účty vytvořené mimo systém Identity & Role Management a tudíž mimo proces.

► NIŽŠÍ MNOŽSTVÍ PRÁCE A MÉNĚ CHYB DÍKY AUTOMATIZACI

Systém pro Identity & Role Management automatizuje všechny procesy a politiky, které jsou se správou přístupových práv spojeny. Nic se díky tomu neopomene, nedochází k chybám a zaměstnanci IT ušetří mnoho času, který mohou věnovat jiným činnostem.

► OCHRANA DAT A OSOBNÍCH ÚDAJŮ

Ve vašich interních systémech se obvykle nacházejí i velmi citlivé osobní údaje zákazníků, jejichž ochrana je povinná ze zákona, či finanční data firmy. Bez systematizace na poli přístupových práv si ale nikdy nemůžete být jisti, že do těchto informací nahlíží jen ti, kteří k tomu mají příslušné oprávnění a odpovědnost. Jistě nechcete riskovat problémy s únikem osobních údajů, ze kterých mohou plynout i velmi vážné soudní spory.

► JEDNOTNÉ PŘIHLÁŠENÍ NAPŘÍČ VŠEMI SYSTÉMY

Určitě to znáte – do každého systému ve vaší firmě mají pracovníci jiné jméno a heslo. Někde heslo musí být dlouhé, někde se musí měnit jednou za tři měsíce, někde platí dlouho to samé. Pracovníci si kvůli tomu hesla nepamatují, píší si je na papírky, ty pak ztrácejí, případně si zapomínají heslo změnit a musí kvůli tomu využívat nákladnou podporu IT. Řešení pro Identity & Role Management zajistí jednotné přihlašovací údaje (single sign-on) napříč všemi systémy. Pracovníci budou mít tedy jedno jméno a jedno heslo, o které se budete starat – nic víc.



KONTAKTUJTE NÁS

AMI Praha a.s., Pláničkova 11, 162 00 Praha 6
Telefon: +420 274 783 239 | E-mail: obchod@ami.cz | Web: www.ami.cz

IDENTITY & ROLE MANAGEMENT



VÍCE O IDENTITY MANAGEMENTU

Identity Management v sobě zahrnuje politiky, procesy a data, prostřednictvím kterých je možné identifikovat uživatele a jeho oprávnění při práci s různými informačními systémy podniku. Základními funkcemi Identity Managementu jsou snadné vytvoření a smazání uživatelských účtů, zajištění schvalovacího procesu a aktivace či deaktivace účtů v operačních systémech, databázích a aplikacích.

ZKUŠENOSTI

Při implementaci aplikace Identity Management 7.1 jsme vyvíjeli nové funkcionality jako např. podpora časového omezení rolí, rekonsiliace rolí, podpora nových atributů a další. Většina těchto funkcionalit byla zahrnuta v nové verzi 8.0. Zkušenosti ukazují, že produkt se vyvíjí jak dle požadavků implementátorů, tak zejména dle požadavků byznysu.

Na obrázku dole jsou zobrazeny dva cyklické procesy z Identity Managementu: Řízení životního cyklu identity definuje, k čemu by měl mít uživatel přístup, a Audit identit ověřuje, k čemu přístup uživatel skutečně má.

VÍCE O ROLE MANAGEMENTU

Role reprezentuje stálou kolekci přístupových práv k jednotlivým systémům. Role se stává důležitým kontrolním bodem, který podniky potřebují spravovat ve všech fázích životního cyklu, tak jako identity. Role Management pokrývá následující oblasti:

- Definice nových rolí přes automatický role mining (automatizovaná analýza, která objevuje úroveň nároku na aplikaci) stávajících rolí.
- Auditorský dashboard se zobrazením stavu certifikace práv napříč celou organizací a všemi aplikacemi.
- Správa role v celém životním cyklu – umožňuje změnu vlastníka role, revize role, přidělení role či deaktivaci role.
- Vytvoření procesu, pomocí kterého bude možné definovat a vytvářet nové role prostřednictvím řídicích postupů použitých pro již existující role.



KONTAKTUJTE NÁS

AMI Praha a.s., Pláničkova 11, 162 00 Praha 6
Telefon: +420 274 783 239 | E-mail: obchod@ami.cz | Web: www.ami.cz