

Rollspel på riktigt

Med en vardag där företag köps, säljs och går samman samtidigt som medarbetare byter avdelning, blir befordrade, tar tjänstledigt eller säger upp sig, är det kanske dags att fråga sig vem som egentligen har koll på din organisations identitetshandling? Lägg därtill utmaningen att i samma miljö hantera exempelvis lösenordsuppdateringar. Är man IT-chef med ambitioner och arbetar i ett större företag, har man mycket att vinna på att så snart som möjligt upprätta en strategi för att hantera sin organisations identiteter – Identity Management (IdM).

Samtidigt, och kanske delvis därför, som större företag skall hantera en allmänt komplex organisationsstruktur skall man klara av att möta allt hårdare myndighetskrav vad gäller god intern kontroll och säkerhet. Om IT-cheferna har att brottas med identitets- och lösenordshandling så faller det på ledningen att förstå konsekvensen av nya lagar och regler som exempelvis Sarbanes-Oxley*.

JÄMFÖR PER AUTOMATIK RÄTTIGHETER MED ROLL

Många företag har hittills valt att möta den nya komplexiteten med manuella, individberoende processer. Förutom att kostnaderna för att underhålla dessa system till slut blir orimliga tycks det i längden omöjligt att på detta vis upprätthålla kraven på säkerhet och klara behovet av att införa nya affärsskapande IT-applikationer.

I grund och botten handlar IdM om vilken roll identiteter skall spela i företaget – hur rätt individ får tillgång till rätt information? I ett Identity Management-system är rollerna knutna till verksamheten och definieras som t ex "konsult", "löneadministratör" eller "säljare". En roll innehåller i sin tur policys som definierar vilka rättigheter olika användare skall erhålla i alla de olika verksamhetssystemen. En lösning som varje dag per automatik jämför givna rättigheter med personens senaste roll. Genom att hantera identiteterna i ett integrerat flöde med exempelvis personal-system blir behörighetskontrollen både tydligare och enklare. När administratören tar bort en användare med tillhörande roller, tas användarens konton automatiskt bort i samtliga system.

TÄNK NYTT UTAN ATT SKROTA BEFINTLIGA SYSTEM

En av utmaningarna inom Identity Management ligger i att skapa en identitetshandlingsprocess som inte försvårar en vidareutveckling av de underliggande verksamhetssystemen. Få företag vill byta ut sin befintliga IT-infrastruktur bara för att kunna implementera ett IdM-system. Det verkar samtidigt som om marknaden varit lyhörd för detta. Som exempel erbjuder Suns produkt "Identity Manager" en lösningsarkitektur som innebär en minimal påverkan på dessa underliggande system.

Investeringarna i den befintliga infrastrukturen kan därigenom utnyttjas på ett optimalt sätt. Peter Lindwall, som arbetar med Identity Management på Inserve, menar att företag med flera verksamhetssystem baserat på olika teknikplattformar och en blandning av gammalt och nytt ofta har särskilt stora behov av att arbeta med IdM. Peter Lindwall igen: "vårt erbjudande täcker hela kedjan från inledande problemanalys fram till implementering och driftsatt system. Vi driver implementationsprojekt med tydliga delsteg, som var för sig löser väl avgränsade problem. Det skapar tydlig nytta, minimerad risk och ger i de flesta fall en återbetalningstid på under ett år."

CASE: IDENT. MANAGEMENT/HENKEL



HENKEL GICK FRÅN EGEN MANUELL LÖSNING TILL INTEGRERAT SYSTEM

Katarina Kreutzfeldt, som arbetar på tyska KOGit, ett IT-konsultföretag som specialiserat sig på Identity Management, berättar hur tyska storkoncernen Henkel löste frågan om identitetshandling.

"Henkel hade tidigare en egen lösning. Ökade krav på flexibilitet och säkerhet gjorde dock att den existerande lösningen ifrågasattes.

Företagsfusioner och nya människor med nya rättigheter drev på utvecklingen. Henkels egna system för identitetshandling saknade vissa kritiska funktioner (audit, reporting, workflow etc) och särskilt uppfattades Internetsupporten som eftersatt. Efter en mycket noggrann utvärdering bestämde sig Henkel för att tillsammans med KOGit använda Suns Java Systems Identity Manager (tidigare Waveset Lighthouse). Det nya systemet byggdes med tydliga krav att kunna hantera de ca 50 befintliga systemen (SAP, Lotus Notes, databaser, AD och LDAP). Eftersom en sån här lösning bara kan fungera om jag har koll på alla system och alla applikationer behöver nya system kunna kopplas på snabbt. Exempelvis är säkerhet något som uppnås endast när alla system blir integrerade."

Hos Henkel förenklades inte bara administrationen av användarrättigheter, även kvaliteten på data förbättrades. Följden av det nya systemet blev sänkta kostnader, en tydligt förbättrad säkerhet samt en snabbare och säkrare service för både kunder och medarbetare. Från beslut till färdig implementering tog projektet ca 8 månader. Katarina Kreutzfeldt framhåller också att en av anledningarna till att hela projektet blev så väl mottaget hos Henkel var att utbildning för IT-administratörerna var en inbyggd del i projektet.

¹ Amerikansk lag stiftad 2002 mot manipulering av bokföring och annan ekonomisk information.

IDENTITY MANAGEMENT - DRIVKRAFTERNA

- Fler integrerade system kräver enhetlig användaridentifiering för att undvika "identifieringsinfarkt".
- Externa krav på säkerhet och rollbaserad identifiering av användare (t ex Sarbanes-Oxley).
- Krav på driftseffektivitet. I framtiden har organisationer inte råd med identitetshandling för enskilda system.
- Krav på användareffektivitet och enkelhet. Exempelvis portallösningar gör att användaren kan röra sig mellan olika applikationer utan inloggning.



www.inserve.se