

Identity Management: Ingen vei utenom

I en bransje som oversvømmes av forkortelser, uttrykk og moteord, er det ikke til å unngå at vi fra tid til annen går glipp av noen. Kun unntaksvis er det imidlertid snakk om noe som er tilstrekkelig viktig til at overseelsen representerer et tap. IDENTITY MANAGEMENT hører hjemme i denne gruppen – men årsaken er sjelden at den er oversett. De fleste IT-personer vi har vært i kontakt med, mener at de har situasjonen under kontroll.

Under kontroll?

Så er sjelden tilfelle. Igjen er imidlertid virkeligheten nyansert og hva som sees, kommer an på øynene som ser. Situasjonen er med andre ord at de fleste tror de har situasjonen under kontroll, mens nærmere undersøkelser viser at så definitivt ikke er tilfelle – dersom vi forutsetter at 'under kontroll' betyr å vite hvor identiteter oppstår, hvem som har ansvaret for deres vedlikehold og oversikt over koblingen mellom dem. Dessuten finner vi kun unntaksvis oppdaterte rutiner som tar vare på det som på dårlig norsk kalles *provisioning* – de systemmessige operasjonene som hører inn under opprettelse, oppdatering og sletting av brukeridentiteter.

Spore til innsats

Det er i manges øyne ironisk at oppmerksomheten rundt styring og kontroll av identiteter kom i søkelyset for alvor først etter at Microsoft for noen år siden lanserte sin Passport-tjeneste. Tjenesten skulle forenkle publikums administrasjon av egne *on line* identiteter ved at hver og én registrerte seg hos Microsoft, som deretter skulle ta hånd om både sikkerhet, oversikt og bruk av ulike identiteter. De negative reaksjonene kom både fra publikum og fra konkurrenter. En gruppe av sistnevnte var raskt ute med å definere og deretter etablere en alternativ tjeneste, og fikk myndighetene i USA med på at Microsofts Passport representerte en trussel – med den følge at Microsoft reduserte ambisjonene og gikk stille i dørene i en periode.⁸

Diskusjonen om Microsofts hensikter og muligheter hører hjemme i en annen sammenheng. Vi er i dette tilfellet opptatt av styring av og kontroll med identiteter: Mens forbausende mange miljøer synes å være av den oppfatning at katalogtjenestene som er innført i løpet av de siste årene har tatt vare på problemet, er det motsatte ofte tilfelle. De fleste har ikke bare én katalogtjener, men en rekke av dem, og situasjonen ligner til forveksling på den vi hadde før katalogtjenestene kom på banen.

⁸ Grupperingen, som kom i stand på initiativ fra Sun og Oracle, bærer navnet Liberty Alliance og har praktisk talt alt som kan krype og gå av navn fra bransjen – med unntak av Microsoft – som enten hovedmedlemmer eller sponsorer. Også flere offentlige institusjoner er å finne blant støttespillerne, for eksempel det amerikanske forsvarsdepartementet.

Besværlige katalogtjenester

Dette er ikke katalogtjenestenes feil. De er nødvendige for å kunne etablere noen form for identitetsstyring. Samtidig er de kun en mekanisme – som vi gjerne skulle ha hatt kun én av, men som konkurrerende leverandører i markedet sørger for at vi må ha flere av. Microsoft forlanger at Active Directory må brukes for å kjøre Windows 2003, mens Oracle Internet Directory må være på plass for at databasene fra samme leverandør skal fungere – og så videre. Derfor blir styring av katalogtjenester en oppgave i seg selv, og en av de første vi må bringe under kontroll på veien frem til en effektiv identitetsstyring.

Organisatoriske utfordringer

En annen fundamental oppgave er å gjennomgå organisasjonen for å finne ut hvor brukeridentiteter finnes i dag, hvor og hvordan de oppstår og hvilke prosedyrer eller regler som eksisterer for å vedlikeholde dem. Om det er aldri så innlysende at prosessen må begynne i denne enden, har det så langt hørt til unntakene at arbeidet med identitetsstyring har strukket seg utenfor IT-domenet.

I de fleste organisasjoner med mer enn noen titalls medarbeidere, viser erfaring at de ansatte har identiteter i 8 sammenhenger eller systemer – herunder 3 IT-systemer/applikasjoner, personalsystem, timeregistreringssystem, lønnsystem og sentralbord/telefonsystem. Hvert sted har sin ansvarlige og sine rutiner for registrering og vedlikehold, og målsettingen er å redusere antallet – aller helst til ett sted og med felles rutiner for vedlikehold.

Utfordringen er ofte større på det organisatoriske nivå enn på det tekniske, fordi noen – kanskje alle – må gi noe for å få noe. Det er ikke til å unngå at enkelte vil føle seg truet eller sin viktighet redusert dersom de skal gi fra seg kontroll i en slik sammenheng. Her er det imidlertid viktig å fokusere på at målsettingen ikke er flytting av ansvar. At slike forandringer forekommer i kjølvannet av prosessen, er riktignok ikke uvanlig, men skjer da som et resultat av avklaringer og omforenede endringer, ikke fordi de var planlagte i utgangspunktet.

Målsettingen er å få data og prosedyrer under kontroll, og å tilby verktøy og tjenester som optimaliserer og forenkler oppgavene for alle involverte. For eksempel er det optimalt at hver enkelt bruker får mulighet til å vedlikeholde informasjon om seg selv i det sentrale brukerregisteret: Hjemmeadresse, telefonnummer, pårørende og så videre. Det er tungvint og bakvendt at andre skal være involvert i registrering og vedlikehold av slik grunnleggende, personlig informasjon. Samtidig illustrerer eksemplet viktigheten av å ha riktige aksesskontrollmekanismer til de ulike dataobjektene: Hva skal kunne leses, endres, sees eller slettes av hvem? Skrekkeeksemplet er naturligvis at vi åpner for individuell endring av egen adresse og telefonnummer, og ved en inkurie gjør det mulig å samtidig endre lønn, trekk eller rapporter fra medarbeidersamtaler.

Slike sikkerhetsmessige forhold er blant hovedårsakene til motstanden mot å etablere sentrale, overordnede katalog- og styringssystemer, spesielt fra personal-siden i organisasjonen. Tilsvarende sikkerhetsmessige argumenter kan imidlertid også anføres i motsatt vei: Uten full kontroll over identitetene, deres 'oppstandelse' og 'tilintetgjørelse', er sjansene overhengende for at uvedkommende – for eksempel tidligere ansatte – får tilgang til informasjon og systemer de absolutt ikke skulle ha adgang til. Faktum er at det finnes langt flere eksempler på sikkerhetsbrudd av denne enn av den første typen.

Sterke drivkrefter

Å få kontroll over interne identiteter er imidlertid ikke den eneste motivasjonen for å introdusere profesjonelle verktøy for identitetsstyring. Behovene for ryddighet vokser i takt med ekspansjonen i bruk av IT-verktøy i alle tenkelige sammenhenger. Her er noen av elementene:

- ✓ Nye brukergrupper skal betjenes og tas hensyn til både praktisk, kvalitetsmessig og sikkerhetsmessig. Kunder, prospects, leverandører, partnere, konsulenter, besøkende og flere – nye kategorier hver med sine krav til rolledefinisjoner og aksesskontroll.
- ✓ Mens antall applikasjoner ikke nødvendigvis øker, vokser deres behov for å spille sammen, hvilket i sin tur aksentuerer kravene til homogene brukerdefinisjoner, rolledefinisjoner og aksesskontroll-lister.
- ✓ Krav fra myndigheter og bransjestandarder hever terskelen for internkontroll og jekker samtidig fallhøyden flere hakk oppover. Forskrifter fra Datatilsynet og EU-kommisjonen er nærliggende eksempler, og sjansen for stikk-kontroller sørger for at full orden må kunne dokumenteres til enhver tid.
- ✓ I denne floraen av identiteter, brukere og roller er etablering og opprettholdelse av tilfredsstillende sikkerhet en eksponentielt voksende utfordring – ikke minst i lys av at nettopp identitetstyveri er den raskest voksende årsaken til innbrudd.

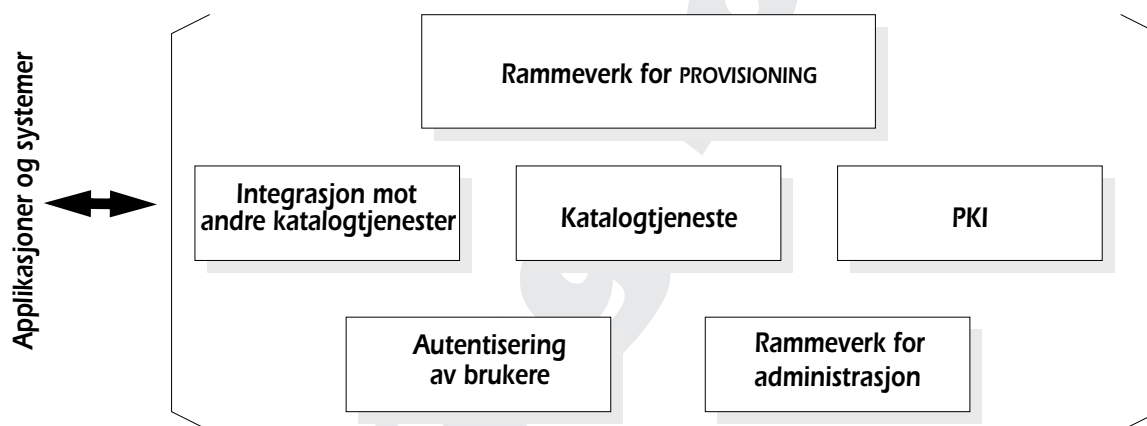
Fra data til PROVISIONING

Å skulle skape og holde orden i dette mangfoldet av systemer, applikasjoner, roller, brukergrupper og krav uten skikkelige verktøy er simpelthen ikke mulig. Dessuten er objektmengden, som vi kan kalle den samlingen variable vi har nevnt hittil, kun toppen av isfjellet. Identiteter, roller og sammenhenger er tross alt ikke noe annet enn data, som skal systematiseres og holdes orden på.

Neste trinn er å sørge for at de underliggende systemene kan forstå og utnytte dataene. At en bruker er registrert har liten verdi dersom hun eller han ikke får tilgang til sine arbeidsverktøy. I mangel av et dekkende norsk uttrykk kalles dette *provisioning* – mekanismer som foretar de nødvendige registreringer og justeringer i applikasjoner og systemer. Nye brukere skal for eksempel registreres i Active Directory for å få tilgang til Windows-ressurser og -tjenester, i et Windows domene for tilgang til eldre Microsoft-systemer, i Oracle for å få tilgang

til databasen, i SAP for å få tilgang til ERP, i Notes – og så videre. I neste tilfelle er det en bruker som skal slettes eller rettigheter som skal endres. Operasjonene må automatiseres for å bli pålitelige, og et moderne *Identity Management* skal dekke også slike oppgaver.

Figur 2 viser hovedelementene i et slikt system – som enkelte leverandører noe pompøst kaller en 'infrastruktur'. Interessen for slike hjelpemidler ble, som vi var inne på innledningsvis, først stimulert av Microsofts Passport-introduksjon. Siden har det dukket opp moderne *Identity Management* produkter fra samtlige store programvareleverandører – CA, Oracle, Novell, Sun, IBM, Microsoft og så videre. Vi skal gå lenger inn i hvilke funksjoner et slikt system bør ha og en del forhold som krever oppmerksomhet ved evaluering av produkter, i neste utgave – i del 2 av denne artikkelen. På de neste sidene skal vi konsentrere oss om ett av grunn-elementene i enhver *Identity Management* løsning: Katalogtjenesten.



Figur 2 Et moderne IDENTITY MANAGEMENT system består av en samling komponenter som til sammen ikke bare skal holde orden på informasjon om brukerne og deres identiteter, men også automatisere oppsett, endring og fjerning av brukere i ulike systemer.

Katalogtjenesten

Som vi var inne på innledningsvis, er katalogtjenester blitt en selvfølgelig del av vår IT-infrastruktur, uten å ha innfridd forventningene til forenkling og effektivisering. Det kan hevdes at vi ikke ville ha klart oss uten tjenestene, men det er samtidig innlysende for de fleste at katalogtjenestenes potensiale er dramatisk underutnyttet. En av årsakene har vi allerede nevnt – at leverandørene er for paranoide (eller mangler selvtillit) til å åpne sine grensesnitt mot reelle eller antatte konkurrenters tjenester. Like viktig er imidlertid at det ikke har eksistert 'lim' – overliggende infrastruktur – som har tatt tak i resten av utfordringen knyttet til administrasjon av brukere, for eksempel *provisioning*, som vi diskuterte ovenfor.

Situasjonen med flere uavhengige katalogtjenere og brukerinformasjon spredt dem imellom kan ha fungert tilfredsstillende i en periode, men er i ferd med å bli en begrensning i stedet for et hjelpemiddel.

Behovet for å få samlet all informasjon under én hatt er påtrengende og voksende. Mens utsiktene til å kunne redusere tallet til én i overskuelig fremtid er små, har muligheten til å etablere automatisk og transparent synkronisering mellom ulike katalog-produkter bedret seg vesentlig det siste året. For eksempel kan Oracles Internet Directory sameksistere transparent med Active Directory via LDAP, med toveis automatisk synkronisering. Tilsvarende funksjonalitet finnes mellom Novells eDirectory og Active Directory. Dessuten, som vi også skal komme inn på i neste artikkel (neste utgave), har flere av *Identity Management* produktene på markedet funksjoner som er til god hjelp for å besørge slik synkronisering.

Flere katalogtjenere trenger med andre ord ikke lenger å bety at samme brukerdata må vedlikeholdes på flere steder. Automatisk synkronisering gjør det mulig å realisere det viktigste kravet for å komme videre i utviklingen: Sentralisering av alle brukerdata til én felles katalog. Ikke bare er dette en forutsetning for å tilfredsstille krav fra offentlige myndigheter, det er også nøkkelen til å etablere et tilfredsstillende sikkerhetsnivå i organisasjonen.

Hver bruker har allerede flere roller i de fleste organisasjoner, for eksempel avhengig av hvor vedkommende er logget inn fra. Antallet roller vil vokse i takt med 'webifiseringen' av applikasjoner og introduksjonen av portaler som generell *front end* til applikasjoner. Denne 'webifiseringen' har for mange positive bieffekter til at den kan stoppes, og argumentene for å starte tilretteleggingen og å utnytte mulighetene er mer enn gode nok til å flytte portalprosjekter oppover mot toppen av prioriteringslistene.

Diskusjonen omkring katalogtjenere og behovet for sentralisering kan videreføres i det uendelige, men følgende punkter representerer essensen i vår sammenheng:

- ✓ Om det ikke lar seg gjøre å redusere antall katalogtjenester til én, så er det et poeng å redusere så mye som mulig. At det ikke var mulig for et år siden betyr ikke at situasjonen er den samme i dag.
- ✓ Bruk den tid og andre ressurser som må til for å etablere effektiv toveis synkronisering mellom de gjenværende tjenestene. Brukerinformasjonen skal finnes i kun én versjon, og skal være konsistent på tvers av alle katalogtjenere.
- ✓ Velg én av katalogene som *master*. Den skal inneholde all informasjon knyttet til en bruker. Andre kataloger kan, men må ikke, inneholde hele informasjonssettet. Unntaket er tjenere som skal være aktive *backups* for hverandre.
- ✓ Sørg for å delegere ansvaret for vedlikehold av informasjon i katalogen så langt ned i organisasjonen som mulig. Dette bidrar til å sikre datakvaliteten og i sin tur til å sørge for at egne kvalitetskrav og offentlige lover og forskrifter overholdes.

Neste utgave

I neste utgave tar vi for oss funksjonalitet og tjenester i moderne *Identity Management* produkter, og diskuterer deres egenskaper, begrensninger og praktiske nytteverdi. Vi skal også komme inn på hvordan våre interne systemer kan forholde seg til Internett-baserte tjenester med tilsvarende målsetting – som Microsofts Passport og tilsvarende fra Liberty Alliance. ■