Identity management: De CD-rom voorbij

Meer dan techniek

Resources moeten meer dan ooit te voren beschermd worden. Het beheer van electronische toegangscodes en toegangsrechten is cruciaal. Dit heet identity management en de belangstelling voor de techniek hiervan, ofwel de identity management tools, is groot. Deze technische tools zijn noodzakelijk maar zijn geen garantie voor succesvol identity management. Sterker nog, ondoordacht invoeren van een nieuw identity management tool is een bedreiging voor de bescherming van resources.

Over de techniek van identity management willen we het hier niet hebben, daar wordt al veel over gepubliceerd. Wel over de noodzakelijke bewustwording voordat de CD-rom met tools wordt uitgepakt. Wat is de impact op de bestaande bedrijfssituatie?

Het identity management procesmodel [zie kader] biedt houvast bij het bepalen van deze impact. Volledigheid van problemen en oplossingen geven we hier niet, wel een handzaam kader voor het ondersteunen van de bewustwording.

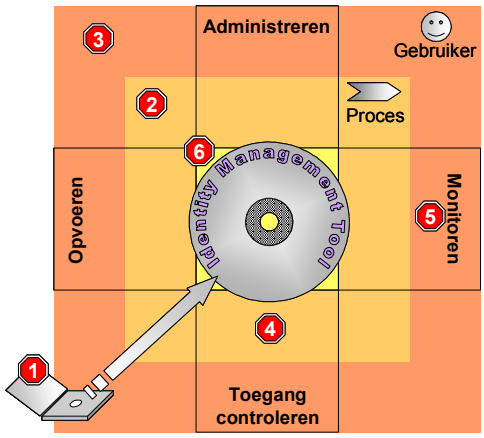
Dat hebben we al

Bedrijven beheren nu ook identiteiten, hebben toegangscontrole en doen al aan identity management. En dat moet ook, want anders zou er geen werknemer of klant toegang krijgen tot zijn applicaties of diensten. Toch willen bedrijven een nieuw Identity Management Tool©, waarom? Omdat het single sign on biedt, omdat het goedkoper wordt, omdat SOX dwingt, of andere zeer gegronde redenen voor een nieuw identity management project.

Een technisch product is gekozen, en dan ..... de CD-rom met het Identity Management Tool© blijkt slechts een deel van de oplossing te zijn. De operationele processen administreren nu al gebruikers, in databases worden al gebruikersnamen en wachtwoorden opgevoerd, gebruikers krijgen toegang tot resources en incidenten worden al opgemerkt. Kortom de bestaande administratie-, opvoer-, toegangscontrole- en monitorprocessen [zie kader] moeten aangepast worden aan het nieuwe IM Tool©. En als processen wijzigen, zullen ook de mensen die volgens deze processen werken anders moeten gaan handelen. Hiermee komen we aan bij de impact op de bestaande organisatie.

Impact van een nieuw IM Tool©

Als het hart van identity management, de techniek wordt vervangen door, of beter gezegd, uitgebreid met nieuwe technologie, dan blijft de de rest van het bedrijf niet automatisch aangesloten.



In het identity management procesmodel wordt de impact op de bestaande organisatie getoond aan de hand van veel voorkomende pijnpunten als bij invoering de aandacht teveel op de CD-rom is gericht.

1. Een systeem erbij

De invoering van een nieuw IM Tool©, is de invoering van een extra IT-systeem: legacy systemen met bestaande access control lists vervallen niet. De nieuwe wereld wordt eerder complexer dan eenvoudiger. Hierin schuilt ook een beveiligingsrisico waar monitoring terdege rekening mee moet houden.

2. Processen moeten verbouwd

De administratie- en opvoerprocessen moeten worden aangepast. Kijk naar een identity management project als het stroomlijnen van het beheer van identiteiten over gedistribueerde databases en het is meteen duidelijk dat processen anders gaan lopen en bij voorkeur geautomatiseerd worden. In de praktijk worden gebruikers opgevoerd zonder goed onderscheid tussen het bijwerken van de klant- of medewerkersadministraties en het opvoeren van de electronische identiteiten in de technische identiteitendatabases. Het is verstandig om het opvoeren van deze identiteiten uit de algemene administratieprocessen te verwijderen en

Largos
Postbus 63
2501 CB Den Haag

Telefoon: 070 – 383 6467
Telefax: 070 – 383 6492
KvK Haaglanden 27245111

over te hevelen naar specifieke identity management processen. Dit voorkomt dat via de achterdeur ook nog identiteiten of gebruikersnamen worden aangemaakt.

Vooraf moet worden nagedacht in hoeverre het administreren van gebruikers centraal of decentraal gebeurt. Wettelijke verplichtingen monden snel uit in centrale uitvoering vanwege de vermeend sterkere controle. Daarentegen levert decentrale uitvoering door direct belanghebbenden in plaats van helpdesk medewerkers de hoogste kwaliteit op: een pleidooi voor gebruikers-selfservice en het aanwijzen van gedelegeerde beheerders gekoppeld aan betrokken managers.

3. Leren en afleren
De medewerkers in het administratieproces krijgen te maken met andere tools en processen en zullen hierin getraind moeten worden. Medewerkers moeten niet alleen iets nieuws leren, maar ook oude gewoontes afleren. Administratieve medewerkers mogen geen persoonlijk contact hebben met systeem beheerders voor het opvoeren van gebruikersnamen en toegangrechten op straffe van inconsistenties in de identiteiten-databases.

4. Single sign-on niet voor alle diensten
Natuurlijk leeft de wens voor single sign-on en dit is bereikbaar, maar wel binnen grenzen. Wat is de scope van single sign-on voor de gebruiker: voor een beperkt aantal diensten, voor alle diensten van dit bedrijf, en ook alle diensten van alle partners? Hoe moet worden omgegaan met gebruikersnamen voor een groep? Wat zegt het informatie beveiligingsbeleid over single sign-on: worden er aparte gebruikersnamen voor risicovolle processen voorgeschreven? De techniek lost deze vragen niet op tijdens een identity management project.

5. Meer veiligheidsrisico's
De start van een identity management project ligt veelal in het efficiënter maken van het administratie proces en het vereenvoudigen van de toegangscontrole bijvoorbeeld met single sign-on. Maar de meeste impact heeft het project op de opvoer processen in de legacy omgeving: de complexiteit van deze wereld wordt niet op voorhand doorzien en leidt tijdens een project tot snelle shortcuts tussen oude en nieuwe processen en tussen oude en nieuwe technieken met alle gevolgen voor de beheersbaarheid van de nieuwe situatie.

De invoering van single sign-on kan door technische koppeling tussen vele portals en toepassingen leiden tot ongewenste toegang tot diensten die voorheen afgeschermd waren. Ook zijn bij single sign-on de consequenties van verlies of diefstal van een gebruikersnaam en wachtwoord veel groter dan voorheen. Serieuze tijden voor monitoring breken aan, al tijdens de realisatie van een identity management project.

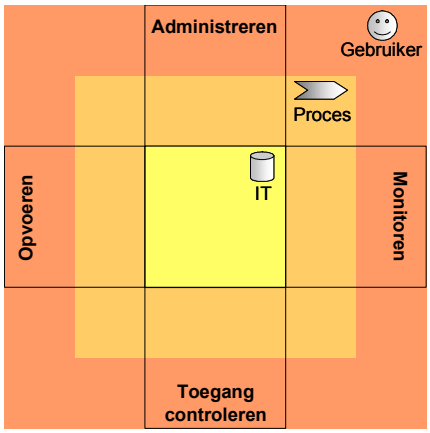
6. Techniek is geen Haarlemmer olie
Voorafgaand aan een identity management project moet vastgesteld zijn wat een unieke gebruikers identificatie is die over alle identiteiten databases heen gebruikt kan worden. In de praktijk blijkt dit heel lastig omdat de huidige identiteiten-databases vervuild zijn met oude gegevens of gebruikers die onder meerdere namen zijn opgevoerd. Het is lastig om met zekerheid te bepalen wie welke rechten krijgt of aan wie nieuwe gebruikersnamen en wachtwoorden heen gestuurd moeten worden. Ook blijken criteria voor het verlenen van toegang tot verschillende diensten niet verenigbaar: voor de ene dienst is controle van het email-adres voldoende en voor een andere dienst blijkt dat ook het betalingsgedrag wordt gecontroleerd. Identity Management Tools© lossen deze problemen spijtig genoeg niet zomaar op.

Een identity management project verwacht input vooraf en niet achteraf. Kennis van o.a. de huidige toegangsregels, bestaande identiteiten, wachtwoord policies, eigenaarschap van resources is essentieel om identity management te verbeteren. Opgepast, de praktijk is anders dan de papieren afspraken. En voordat je het weet is een identity management project ook een nieuw beleid aan het formuleren.

Als technieken en standaards ruim voorhanden zijn, blijkt in de praktijk de aanpassing van de bestaande organisatie de bottle-neck bij invoering. Dit is niet uniek voor identity management en is vaker voorgekomen zoals bij nauw gerelateerde technieken als Public Key Infrastructures en digitale handtekeningen.

Conclusie
Identity management projecten zijn niet louter technisch projecten: de uitdaging ligt juist in het integreren van techniek en organisatie waarbij processen en mensen moeten veranderen. De kern van een goed identity management project zit in het doorgronden van de huidige operationele processen.

Het identity management procesmodel
Identity management wordt gedefinieerd als het toekennen, beheren en gebruiken van electronische identiteiten, om veilig en gecontroleerd toegang te geven tot specifieke resources. Deze definitie toont al een natuurlijke opdeling in de vier identity management hoofdprocessen: Administreren, Opvoeren, Toegang controleren en Monitoren.



- *Administreren:* Het toekennen (of intrekken) van een electronische identiteit en toegangsrechten aan geïdentificeerde gebruikers die met naam en toenaam worden geadministreerd. Een electronische identiteit is vaak een gebruikersnaam hoewel inlog-tokens steeds vaker voorkomen. Identificatie van gebruikers kan meer of minder sterk gebeuren; zwak is bijvoorbeeld een email-adres controle en sterk is een fysieke paspoortcontrole. Onder administreren valt ook het beheer van policies voor het toekennen van rechten en het vaststellen van de condities waaronder wel of geen toegang wordt verleend.
- *Opvoeren:* Na administratie van de electronische identiteit moet deze met de beoogde rechten opgevoerd (of afgevoerd) worden in de technische identiteiten databases. Vaak zijn deze databases per platform of toepassing ingericht. Beheerders met hoge systeemrechten, zoals system administrators, zorgen hiervoor. Ook het synchroon houden van de identiteiten-databases, bijvoorbeeld in geval van wachtwoordwijzigingen, valt onder dit proces.
- *Toegang controleren:* De toegangscontrole waakt over de resources. Alleen na geslaagde authenticatie én autorisatie wordt een gebruiker toegang verleend. Als een gebruiker na het invoeren van zijn gebruikersnaam en wachtwoord goed wordt bevonden, kan hij zijn rechten effectueren.
- *Monitoren:* Onterecht opgevoerde of achtergebleven identiteiten en rechten of het frauduleus gebruik van identiteiten moeten worden opgespoord en gerapporteerd. Alle processen en de inhoud van de identiteiten databaseses worden continu gemonitored.

Van buiten naar binnen zijn in het model de gebruikers, de processen en de IT met identiteiten databases, als aparte lagen geschetst in alle vier de hoofdprocessen. Het model toont belangrijke interacties tussen de hoofdprocessen onderling én de interacties tussen de mens-, proces- en IT-lagen. Onvoldoende begrip en afstemming van deze interacties is een bron voor inconsistenties, niet verwijderde usercodes of incorrecte rapportages.

Hoewel de gebruikte terminologie kan afwijken, hanteren leveranciers en standaards een indeling van identity management systemen die past in het geschetste model.

Wim Geurts en Guido Bezemer zijn consultant bij Largos. Largos is het adviesbureau voor informatie-beveiliging en risicobeheersing sinds 2001.
Contact: wim.geurts@largos.nl of www.largos.nl