PvIB Expertbrief – Juli 2012

Access management (Deel 4: Beheer en gebruik)

ISSN 1872-4876, jaargang 8 – Nr. 1

Peter Hoogendoorn

Jean-Pierre Vincent

Karin van de Kerkhof

Jan-Roel Löwenthal

Karel van Oort

Piet Kalverda

Bert van Ingen

Wiyaykumar Jharap

Peter Lucas

Johan van Westeneng

Aaldert Hofman

Jaap Scheepstra

Renato Kuiper

Pagina

2 INLEIDING EN SITUATIESCHETS

4 DE ONDERZOEKSVRAGEN

6 CONTEXTUELE ACCESS MANAGEMENT ASPECTEN

11 ORGANISATIE ASPECTEN

15 INFORMATIE STRUCTUREN

18 SERVICES EN TOOLING

21 INFRASTRUCTUUR

23 CONCLUSIES EN VERVOLG

24 LITERATUURLIJST

2

INLEIDING EN SITUATIESCHETS

Aanleiding

Steeds meer bedrijven buigen zich over identity- en access management (IAM) vraagstukken. Deze vraagstukken zijn in essentie vaak dezelfde, alleen verschillen de bedrijfssituaties en daardoor de oplossingsrichtingen. Om te voorkomen dat 'AM-wielen' (AM = Access Management) opnieuw worden uitgevonden, worden deze vraagstukken door experts geformuleerd en worden aanpak- en oplossingsrichtingen uitgewerkt in 4 expertbrieven, waar deze de laatste in deze serie van is. Hierdoor kan de kennis op effectieve wijze worden hergebruikt.

Aanpak

Access management (AM) is complex. Het raakt immers alle medewerkers en in sommige gevallen leveranciers en klanten of partners die een relatie hebben met de organisatie op het gebied van logische en mogelijk fysieke toegangsbeveiliging. Om hiervan toch een beeld te kunnen weergeven in expertbrieven, is het onderwerp in vier hoofdgebieden opgesplitst die ieder worden uitgewerkt in een expertbrief. In Bijlage 1 is beschreven hoe deze opsplitsing is uitgevoerd.
Deze expertbrief behandelt deel 4, wat de huidige praktijk inzake access management is en wat verbetertrajecten nu praktisch gezien precies hebben opgeleverd. Om tot deze expertbrief te komen is een zogenaamd kapstokdocument opgesteld met vragen over de access management-situatie in alle gelederen van een organisatie. In de werkgroep-sessie zijn deze onderwerpen besproken en hebben de betreffende specialisten hun inbreng gegeven die is weergegeven in deze expertbrief.

Scope

De scope van deze expertbrief richt zich op het access management deel van IAM. Identity management is buiten scope. Beiden kunnen echter niet zonder elkaar, waardoor het maken van scheiding lastig is. Het is duidelijker om aan te geven dat er geen aandacht wordt besteed aan identificatie- en authenticatie-oplossingen, beheer en controle op smart-card-oplossingen, SSO-oplossingen en authenticatiemechanismes om te controleren of 'je bent wie je zegt dat je bent'. In deze expertbrief gaat de aandacht uit naar wat nodig is voor het verstrekken van autorisaties: beleid, organisatiestructuur, architectuur, processen, bemensing, administratie en (technische) (tooling) middelen.

Doelstelling

De expertbrief heeft tot doel een hulpmiddel te zijn bij het implementeren of verbeteren van een access management organisatiestructuur, beheeromgeving en mogelijk al lopend project/traject. De expertbrief formuleert per onderwerp aandachtspunten waarvan de lezer zelf kan beoordelen of deze in zijn situatie van toepassing zijn, en hoe deze in zijn situatie kunnen worden toegepast.

Definitie

Meestal worden Identity- en Access Management (IAM) in één adem genoemd omdat deze begrippen sterk aan elkaar zijn gerelateerd. Ter afbakening van het begrip access management, gebruiken we de volgende definities:

Access management (AM) is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van systemen en informatie te faciliteren, beheren en controleren.

Identity Management (IDM) is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om van actoren (als gebruikers en systemen) de identificatie en authenticatie te faciliteren, beheren en controleren.

Toelichting op access management:
Access management betreft het regelen van de toegang en de soort toegang van een subject (bijvoorbeeld een medewerker, systeem, service, etc.) tot een object zoals (bijvoorbeeld data, databron of service). In beide gevallen moet worden vastgesteld of het betreffende subject het recht heeft om bij het object zoals bijvoorbeeld de databron te komen (de resource mag de data inzien of muteren[1]) of de service mag gebruiken (bijvoorbeeld: is er een licentie voor de resource beschikbaar). In een enterprise-omgeving gaat het hierbij om veel rechtenverstrekkingen en de controle daarop (schaalgrootte). Daarom loont het zich om de uitvoering daarvan efficiënt in te richten door middel van helder beleid, strakke processen, juiste bemensing met de bijbehorende taken, verantwoordelijkheden en bevoegdheden, correcte administraties en goede (technische) hulpmiddelen.

Totstandkoming expertbrief
Deze publicatie is het resultaat van de 4e expertsessie ‘access management’ en is tot stand gekomen met medewerking van de genoemde personen op de voorpagina (zie voor meer achtergrondinformatie bijlage 2).

Initiatiefnemer van de ‘access management’ expertsessies is Jean-Pierre Vincent. Samen met Aaldert Hofman, Bart Bokhorst en Ben Elsinga is de initiële probleemstelling geformuleerd. Deze is verder uitgewerkt door het organisatiecomité.

De organisatiecomitérollen van deze expertbrief zijn als volgt ingevuld:

Probleemeigenaar:	Karin van de Kerkhof
Facilitator:	Jan-Roel Löwenthal
Co Facilitator:	Jan-Roel Löwenthal
Ghostwriters:	Jean-Pierre Vincent en Peter Hoogendoorn

[1] Onder muteren wordt hier verstaan het creëren, verwijderen en wijzigen van data.

4

DE ONDERZOEKSVRAGEN

De praktijk: In deze vierde expertbrief wordt de operatie van access management, zoals deze heden ten dage in de praktijk wordt uitgevoerd, beschreven. Dit betreft de hele scope van access management in alle gelederen van het bedrijf. Dat betreft zowel de governance, security-invulling, de ervaringen in de business, beheerrollen, operationele uitvoering en ervaringen met ondersteunende tooling (functioneel).

Probleemstelling voor de expertbrief "Access Management in de praktijk"

De kernvraag voor deze sessie is: Hoe ziet een AM-beheerorganisatie er in de praktijk uit? Dat betreft o.a: hoe ziet de organisatie eruit, welke processen worden onderkend, welke spelers (rollen, taken&verantwoordelijkheden&bevoegdheden) zijn benoemd, welke hulpmiddelen worden gebruikt, hoe worden architectuur en security aangelijnd, maar ook wat zijn de standaard compliance issues en hoe wordt omgegaan met outsourcing, cloud, etc? Dit zijn voorbeelden van de vraagstukken die zullen worden uitgewerkt.

Actuele vormen van lijnorganisatie en proces-inrichtingen zullen worden belicht. Als voorbeeld is figuur 1 gebruikt. Hierin staan generieke organisatie-elementen en processen benoemd voor AM. Naast aspecten m.b.t. de lijnorganisatie zelf, wordt ook gekeken naar de consequenties van een geïmplementeerd AM-concept, bijvoorbeeld voor businessprojecten die autorisatiemanagement raken. Zo zal de ontwikkeling van bijv. applicaties zich naar het AM-beleid moeten richten of zal het uitrollen van een nieuwe applicatie in samenwerking met o.a. de AM-organisatie moeten gaan verlopen. Tevens komt het borgen van access management in de veranderprocessen van de organisatie aan bod.
Ook wordt gekeken naar de voordelen van een goed ingericht/geïmplementeerd AM-concept, wat bijvoorbeeld naar voren komt bij reorganisaties (als outsourcing). Omgekeerd kunnen reorganisaties (intern of overnames/afsplitsingen) ook weer effect hebben op delen van het AM-concept en/of de AM-organisatie.

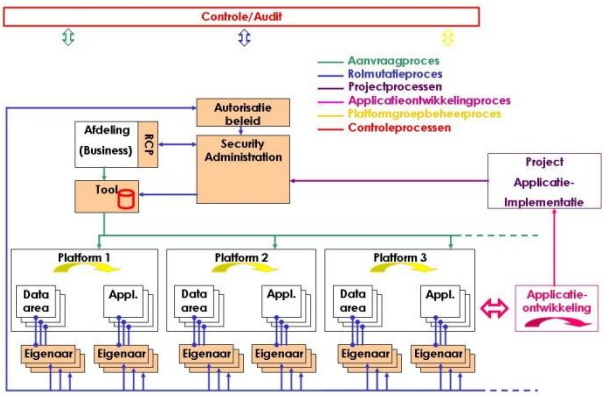


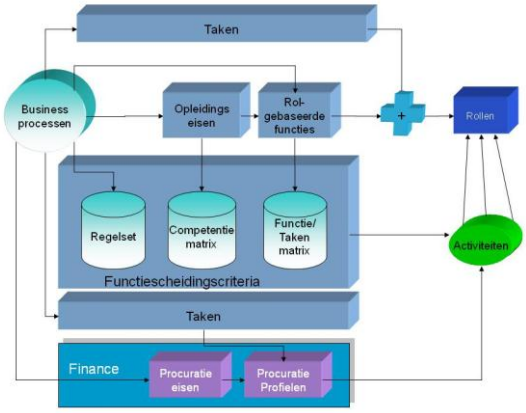
Fig. 1. Organisatie en processen

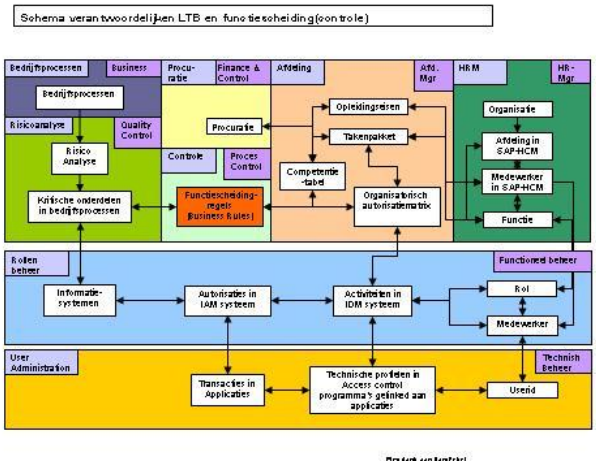
In tegenstelling tot de vorige expertbrieven waarbij het theoretische aspect een grote rol speelde is in deze vooral naar praktische ervaringen gekeken.

- Welke voordelen hebben AM-implementaties nu in de praktijk wel en niet opgeleverd;
- Wat is in de praktijk een probleem gebleken;
- Hoe moeten we resultaten zien in relatie tot de businesscase en welke ervaringen met beschikbare tools zijn er opgedaan (blijft beperkt tot functionele beschrijvingen van de ervaringen, het gaat niet om toolnamen) die in de eerdere sessies niet benoemd zijn?

Samenvattend zijn de vier hoofdvragen voor deze sessie:

1. Hoe zien AM-organisaties er in de praktijk uit en welke ervaringen zijn opgedaan, zowel intern als extern (i.g.v. federatieve oplossingen)?
2. Welke consequenties/gevolgen/mogelijkheden/impact heeft/biedt een AM-implementatieproject op de bestaande AM-organisatie?
3. Is beschikbare tooling wel ideaal, welke functionaliteit ontbreekt altijd, is moeilijk te implementeren, welke informatiebronnen werken goed en niet goed?
4. Welke beoogde voordelen (benefits) zijn daadwerkelijk gerealiseerd?





6 CONTEXTUELE ACCESS MANAGEMENT ASPECTEN

1.1. Visie & strategie

Visie en strategie zijn verbonden met de lange termijn en zouden op de korte termijn niet snel veranderd moeten worden. In de dagelijkse operatie wordt zelden het vertrekpunt vanuit de visie en strategie meegenomen in belangrijke besluitvorming. Dat komt enerzijds omdat er weinig richtinggevend beleid is. Anderzijds is dat wel een succesfactor als het (middel)management dit wel zou doen als het er wel is en eisen dat het er komt als het er niet is. Een middel om dit dichterbij te brengen is de visie en strategie te koppelen aan één of meer directe bedrijfsdoelen. Benoem triggers die teruggrijpen op de visie en strategie.

Een praktijkvoorbeeld met het nieuwe werken.

Het nieuwe werken is een bedrijfsstrategie om met minder kantoorwerkplekken en flexibele inzet van personeel tot kostenreductie en meer tevreden personeel te kunnen komen. Een voorwaarde daarvoor is de inzet van mobile devices die groeien in mogelijkheden en daarmee in complexiteit. De ontwikkelingen gaan zo snel dat bedrijven niet meer in staat zijn deze devices zelf in te kopen en voldoende beveiligd in te zetten. De medewerkers willen zelf hun vertrouwde privé apparaat meenemen en daar ook zakelijk mee kunnen werken. Het ‘bring your own device’ (BYOD) beleid is daar een uiting van. Daarmee wordt krachtige apparatuur met een vreemde signatuur toegelaten op het bedrijfsnetwerk en er komen bedrijfsgegevens op te staan. De meeste bedrijven hebben geen goede gegevensclassificatie ingericht, waardoor correcte autorisatieregels lastig te implementeren zijn (wat mag je wel en wat mag je niet op je mobile opslaan). Vanuit de bedrijfsstrategie zou er meer aandacht moeten komen op het wel goed inrichten van gegevensclassificatie. Het access management zou moeten worden uitgebreid met toegang verlenen tot bedrijfsapplicaties die afhankelijk zijn van plaats en device, zodat de business eigenaren kunnen besluiten welke applicatie in welke omgeving en met welk device mogen worden ontsloten. Dit is een uitbreiding op de gangbare access management functies en wordt ook wel dynamische rol toewijzing, attribuut- of contextgebaseerd autoriseren genoemd.

Hou ook dit praktisch en voer een risicoanalyse uit over alle aspecten en beschouw de aanwezige context en content. Is het bijvoorbeeld toegestaan om financiële transacties via een iPad app in de trein te kunnen goedkeuren? (Content = financiële administratie, context is in een niet gecontroleerde omgeving, risico is het bekend worden van de financiële positie van een bedrijf door personen die meekijken).

HIGHLIGHTS
Vanuit de operatie naar Visie &Strategie (V&S).

- Bij significatie veranderingen in het bedrijf (nieuwe processen, applicaties, afdelingen) afwegingen rond autorisaties meenemen.
- Nieuwe ontwikkelingen zoals tablets, social media, cloud zijn alleen goed mogelijk als gegevensclassificatie is geregeld.

Vanuit Visie & Strategie naar operatie:

- Breng wijzigingen in de V&S ook onder wijzigingsbeheer, zodat de consequenties voor de operatie goed worden door vertaald en gecommuniceerd.
- Veranderende business (overnames etc.) betekent vaak herziening van V&S.
- V&S is niet verantwoordelijk voor inhoudelijke samenhang en keuzes, daarvoor is de Enterprise Architectuur. Waak voor al te gedetailleerde visie statements.

1.2. Principes & Enterprise Architectuur

Principes die noodzakelijk zijn om Access Management structureel goed te kunnen borgen zouden moeten worden door vertaald in de Enterprise Architectuur (EA). EA wordt vaak uitgemodelleerd zonder rekening te houden met AM-principes waardoor de resulterende AM-architectuur verwordt tot iets wat eraan geschroefd moet worden in plaats van AM als volledig en volwaardig element te integreren in het geheel.
Een voorbeeld zal dit duidelijk maken. Stel dat je in je CRM-systeem onderscheid zou willen maken tussen ‘klanten met specifieke doelbinding’. Dan kun je er een totale verzameling klanten van maken en die door middel van ingewikkelde autorisatieschema’s scheiden, of je kan die klanten in meerdere logische mandanten/partities/views onderbrengen waardoor het autorisatieschema er ineens veel logischer uit komt te zien. Wat de beheer(s)baarheid zeker ten goede komt.

EA is vaak wel beschreven maar is niet geborgd in de lijn zodat de daar beschreven principes en richtinggevende indeling niet structureel wordt gevolgd. Zorg ervoor dat het team dat zich bezig houdt met Access Management beslissingsbevoegdheid krijgt in de projecten, waardoor het volgen van de AM-principes kan worden afgedwongen. De legacyproblematiek maakt dit ingewikkelder omdat legacy vaak niet onder architectuur is gebouwd en AM daar geen rol in heeft gespeeld.

Waar in projecten en grote veranderschema’s de EA sneller een volwaardige rol wordt toebedeeld is dat niet zo in de changes die vanuit de lijn worden gestuurd. Change management zou in die zin ook volwaardig moeten worden getoetst op EA geschiktheid. AM dient een plaats te krijgen in het change management / wijzigingsbeheer proces.

HIGHLIGHTS
Vanuit de operatie naar principes en EA:

- Koppel de werking van principes en EA ontwerpcriteria terug aan EA vanuit de operatie. Zorg ervoor dat deze goed worden vertaald in een architectuurontwerp en pas niet de operatie aan buiten de architectuur.
- Betrek EA bij een AM-project. Zonder een gedegen EA zijn AM-projecten lastiger uit te voeren.

Vanuit principes en EA naar operatie:

- Breng wijzigingen in de EA onder wijzigingsbeheer, zodat de consequenties voor de operatie goed worden door vertaald en gecommuniceerd.
- Maak in het begin een aparte rubriek voor AM-principes en vertaal die integraal door in de Enterprise Architectuur.
- Betrek een (solution) architect bij een AM-project.
- Mogelijke KPI: #AM-principes (meer dan 20 dan zijn het teveel principes)

1.3. Beleid & Governance

Beleid en Governance zijn met elkaar verbonden en hebben sterke invloed op de directe dagelijkse praktijk. Beleid, en zeker daar waar het direct is afgeleid van normen en / of wet- en regelgeving, zou stabiel moeten zijn en sterk richtinggevend. Toch is dat niet altijd de ervaring. Beleid wordt vaak naar operationele werkinstructies vertaald waarbij onjuiste interpretaties van het beleid leiden tot een verkeerde toepassing van het beleid in de dagelijkse praktijk. Een voorbeeld is het door managers laten controleren van de toewijzing van rollen aan medewerkers, waar managers totaal geen belang bij hebben voor de dagelijkse operatie. De controle wordt wel uitgevoerd maar geeft niet die kwaliteit die het vanuit een Governance oogpunt zou moeten hebben.

Beleidsuitspraken zouden moeten worden meegenomen in de Enterprise Architectuur en principes. Beleid vormt ook de basis voor de Governance en de rapportages. Governance zorgt voor het aantoonbaar “in-control” zijn van de organisatie. Rapportages zorgen voor het overzicht en de aantoonbaarheid. In de praktijk worden rapportages vaak toegesneden op de auditpraktijk om de auditors tevreden te houden. Dat is echter niet de juiste reden. In feite willen auditors dit ook liever niet, die willen een organisatie zien die “in-control” is.
Hier wordt een eerste indicatie gegeven van de volwassenheid van een organisatie. Van meet af aan is rapportage het belangrijkste element om AM zichtbaar en tastbaar te maken naar de stakeholders. Naarmate een organisatie een meer volwassen stadium heeft bereikt zal de rapportage steeds beter toegesneden zijn op de kwaliteit van de te leveren (IAM) producten en diensten en daardoor de auditors veel beter in staat stellen controles uit te voeren.

Naarmate de volwassenheid toeneemt, is de organisatie veel beter in staat zich aan nieuwe regels van toezichthouders, auditors aan te passen zonder de kwaliteit van de dagelijkse operatie aan te tasten. De aanpassingen zullen dan structureel geïntegreerd worden of afgeleid worden van de Enterprise Architectuur. Er kunnen issues worden afgeleid, gekoppeld aan managers. De issues kunnen op hun beurt een workflow triggeren.

In onze sessie kwam naar voren dat reviews op het geheel aan beleid, architectuur, rapportages en uitvoering daarvan (en de gemeten successen) niet of nauwelijks worden uitgevoerd. Er zijn geen ‘rust’ momenten waar dit wordt uitgevoerd. Toch loont dit de moeite, de kwaliteit van het geheel wordt er beter van en niet in de laatste plaats om de betrokkenheid van de medewerkers die aan de basis staan te verbeteren.

HIGHLIGHTS
Van Beleid naar dagelijkse operatie:

- Zorg ervoor dat beleidsveranderingen door vertaald worden in de dagelijkse operatie.
- Zorg ervoor dat beleidsveranderingen worden getoetst tegen de EA.
- Zorg voor ‘rust’- momenten waarop het geheel aan beleid, controlepraktijk en operatie wordt geëvalueerd zodanig dat alles weer met elkaar in lijn kan worden gebracht.
- Leid beleid zoveel mogelijk af van openbare, algemeen geaccepteerde standaarden.
- Laat het totaal van beleidsdocumenten en governanceprincipes auditen voordat wordt overgegaan tot het implementeren daarvan.
- Mogelijke KPI’s: #gebruikte openbare standaarden; Goedkeuring door management.

Van dagelijkse operatie naar Beleid:

- Voorkom dat operationele situaties tot ondoordachte beleidsaanpassingen leiden.
- Breng RACI / TVB aan in het beleid op basis van operationele werkbaarheid.
- Breng scheiding aan tussen beleid en beleidsuitvoering middels uitzonderingsinstructies die gelden in speciale situaties (vb. Complexe wachtwoorden zijn lastig omdat bij Windows de combinatie “+e → ë en op de iPad wordt deze combinatie gewoon “e. Nog maar niet te spreken van legacy systemen).

1.4. Methoden & Standaarden

Methoden en standaarden zijn er in overvloed. Het is zaak de juiste methode te kiezen, die toepasbaar te maken voor het bedrijf en vooral daarbij de praktische insteek te kiezen. Binnen het vakgebied gaan de ontwikkelingen snel en het gevaar van verlamming door al die veranderingen is aanwezig “Paralysis through Analysis”. Een voorbeeld hiervan is de RBAC discussie. Rol gebaseerd autorisatiebeheer is op het eerste gezicht een logisch model maar de praktijk is een stuk weerbarstiger. Het is zaak het autorisatiemodel/rollenmodel goed toe te snijden op de eigen organisatie en daarna de focus daarop te zetten en deze vast te houden. Kijk daarbij goed wat in de organisatie speelt, als de organisatie (groot of klein) uitstekend georganiseerd is en procesgericht werkt, kunnen de resulterende rollen en procesgang simpel gehouden worden.

Een heterogeen IT-landschap is vaak een struikelblok om AM in te voeren. Maak hier een keuze naar de toekomst en organiseer een work-around voor de niet toekomst vaste(re) systemen. Daar wordt het model simpeler van. Denk aan verschillende type rollen zoals automatisch op basis van functie/organisatie afhankelijke rollen en tijdelijke (project) rollen. En denk aan hiërarchische afhankelijkheid van rollen en regels onderling. Uit diverse ervaringen blijkt dat de sturing die er aanvankelijk in het project wel was later verwaterde. Als je de succesvolle implementaties bekijkt dan lijken er twee succesvolle strategieën:

1. Lever als project alles in een keer compleet op aan een deel van de organisatie en realiseer daarna het volgende bedrijfsonderdeel. Het project loopt wel langer, althans dat spreek je gelijk eerlijk af in het begin, omdat je niet alles voor de gehele organisatie tegelijk doet zullen de kosten meevallen en er zijn gelijk resultaten te zien terwijl het bedrijfsonderdeel dat is opgeleverd andere bedrijfsonderdelen zal motiveren. Na de eerste oplevering kan je de externe krachten wegsturen en kan je het alleen verder af. Tenzij er capaciteitsgebrek is.

2. Lever een eerste werkende applicatie op die de basisfunctionaliteit levert voor de gehele organisatie. Ga vervolgens de bedrijfsonderdelen aansluiten met de business specifieke rollen.

De basis van beide strategieën ligt wel in het centraal bekostigen van het project. In de exploitatiefase kan doorbelasting naar de bedrijfsonderdelen worden ingericht. Dat moet dan wel tijdens de project opstart al geborgd worden met de opdrachtgever(s).

AM-projecten duren vaak lang en zijn inherent complex. Gedurende de looptijd van die projecten droogt vaak de geldstroom ineens op waardoor het model niet afgemaakt kan worden en er geen goede functionaliteit wordt geboden aan de gebruikers. Kernvraag hierbij is hoe dit kan worden voorkomen of moet er gewoon een leidend principe zijn (zie AM expertbrief nummer 3) dat simpelweg stelt dat een AM-project een aantal minimale

10

deliverables heeft om een succesvolle basis te generen voor een volwassen AM in de organisatie?

Zorg ervoor dat zoveel mogelijk gebruik wordt gemaakt van open autorisatie en authenticatie standaarden.

HIGHLIGHTS
Van methoden en standaarden naar de dagelijkse operatie:

- Kies een standaard en maak op basis daarvan een werkbaar model voor de dagelijkse operatie.
- Hou vast aan een eenmaal gekozen methode en/of standaard.

Van de dagelijkse operatie naar methoden en standaarden:

- Laat de dagelijkse praktijk niet steeds de gekozen richting ter discussie stellen, stay focussed.

ORGANISATIE ASPECTEN

2.1. Organisatiestructuur

Access Management kent twee aspecten die van de organisatiestructuur afhankelijk zijn. Enerzijds is de huidige organisatiestructuur een gegeven dat in het autorisatieschema moet worden ingebracht (organisatie rollen die toegang geven tot applicaties / directories / links naar (interne) sites die binnen een specifieke organisatie nodig zijn). Anderzijds raakt het borgen van de rollen de gehele organisatie. Immers veranderingen in de organisatie zullen veelal aanpassingen in de rollen vereisen. Dat is meteen een reden om de rollen zo te kiezen dat organisatiewijzigingen zo min mogelijk vat hebben op de inhoudelijke rollen.
De business heeft vaak andere belangen die wijzigingen in de organisatie sturen. Zorg ervoor dat Access Management aspecten ook deel uitmaken van de voorgenomen organisatieverandering. Betrek het kunnen definiëren van heldere functiescheidingen bij het definiëren van een nieuwe organisatiestructuur. Een rol zou vrij moeten zijn van functiescheidingsconflicten. Soms is dat niet goed mogelijk, zorg er dan voor dat met behulp van rules aanvullende zaken worden gemodelleerd (bijvoorbeeld bij procuratierechten).

Het inrichten van een meer abstract Governancemodel kan hierbij behulpzaam zijn omdat daar de benodigde rapportages en bevoegdheden worden gedefinieerd. Ook Auditors en toezichthouders zijn hiervoor een goede bron.

Laat de last daar waar die hoort. HR moet zorgen voor een deugdelijke personeels-administratie; als daar vervuiling in is ontstaan: laat HR dat dan oplossen. Of meer abstract geformuleerd: de bronnen die voor Access Management worden gebruikt zullen aan kwaliteitscriteria moeten voldoen, dat betekend in veel gevallen dat de bestaande kwaliteit onvoldoende is en moet worden verbeterd.

HIGHLIGHTS

- Draag er zorg voor dat organisatorische wijzigingen zo min mogelijk gevolgen hebben op de inhoud van de rollen. Sluit zoveel mogelijk aan bij de bedrijfsprocessen.
- Verantwoordelijkheid voor goede rollen ligt in de lijnorganisatie. Het is belangrijk deze verantwoordelijkheid vanaf het begin goed mee te nemen.
- Ontwikkel samen met de business een goed governancemodel, daardoor worden taken bevoegdheden en verantwoordelijkheden meteen duidelijk.
- Mogelijke KPI's: #rollen die niet gebaseerd zijn op organisatiestructuren; #rollen gebaseerd op bedrijfsprocessen; #projectrollen.

2.2.Taken, bevoegdheden & verantwoordelijkheden

Taak/functiescheiding matrices zijn lastig uit organisaties te krijgen, wie voert welke taak uit en heeft daarin welke verantwoordelijkheid en welk mandaat/volmacht/procuratie. Vanuit die gegevens kunnen dan functiescheidingsmatrices en mandateringsmatrices worden opgesteld waar het traditionele: opvoeren, registreren en controleren worden gescheiden en ook als autorisaties onderscheiden kunnen worden. Een handige vuistregel is te beginnen met functiescheiding in te voeren daar waar het echt nodig is zoals bij de excasso afdeling. Daar gaat geld naar buiten en daar zijn controles noodzakelijk. Door het scheiden van autorisaties van een rol waarmee excasso opdrachten kunnen worden aangevraagd, het controleren van de aanvraag en daarna het daadwerkelijk uitbetalen, wordt fraude tegengegaan. Dit type

eenvoudige en door het management te begrijpen en te sturen functiescheidingen zijn van belang.
Voor Access Management liggen hier de grote uitdagingen. Het vaststellen van de juiste functiescheidingsmatrices op basis van de taken die worden uitgevoerd gecombineerd met de verantwoordelijkheden die men heeft zullen moeten leiden tot juiste rollen. Dit kan duur zijn als men dit voor alle onderdelen tot het kleinste detail wil modelleren. Praktisch blijven is hierbij het devies met die opmerking dat de werking van deze functiescheidingsmaatregelen wel moet worden aangetoond.

Moderne context – sensitieve AM-oplossingen kunnen ook rekening houden met het kunnen toewijzen van rollen op basis van opleidingseisen of procuratiebevoegdheden. Hou ook hier de regel aan dat eenvoud de sleutel is tot een adequaat beheer daarvan. Ingewikkelde vaak verouderde procuratiereglementen kunnen dit verhinderen.

Deze rollen zullen door goed opgeleide beheerders moeten worden onderhouden. Er zijn een veelheid aan veranderingen die invloed hebben op de rollen. Rollenbeheer zou idealiter moeten zijn geborgd in alle veranderprocessen in de business. Van een eenvoudige wijziging in functie tot complete reorganisaties. Bijvoorbeeld in de feasibility fase van een project. De AM-beheerders dienen dan ook met voldoende mandaat te kunnen opereren. Een eenvoudige maar duidelijke RACI waarin dit is vastgelegd kan hier helpen.
In een gecentraliseerd AM-proces zal er een workflow worden gedefinieerd voor het aanvragen, wijzigen, intrekken etc.. van rollen. Deze workflow kan worden gebruikt om goedkeuringsproces te automatiseren. Dit goedkeuringsproces dient wel in goed overleg met de business worden gemodelleerd. Acceptatie van dit proces is voorwaardelijk voor het slagen van AM. Immers dit proces zal de meest belangrijke interface met de AM wereld zijn. Een proces waarbij de managers (eigenaar en/of lijn) periodiek controleren of de toegekende autorisaties nog valide zijn blijft onontbeerlijk.

HIGHLIGHTS

- Richt een beheerorganisatie in met aparte gespecialiseerde rollenbeheerders.
- Hou functiescheiding eenvoudig en herkenbaar.
- Borg rollenaspecten in alle wijzigingsprocedures in de organisatie. Vrijwel alle aanpassingen in bedrijfsprocessen, organisatie en inrichting hebben gevolgen voor AM. Denk aan een eenvoudige, duidelijke RACI.
- Voorkom vervuiling door het tijdig intrekken van tijdelijk uitgegeven rollen.
- Acceptatie van de business in de workflow processen is van wezenlijk belang.
- KPI’s: #tijdelijke rollen; #rol wijzigingen buiten afgesproken procesgang; #escalaties in toewijzing rollen.

2.3. Processen (business en beheer)

Er zijn twee principieel verschillende autorisatieprocessen. Het toekennen van rollen aan personen (in-, door- en uitstroom) en het inhoudelijk samenstellen van de rollen met respect voor de aan te brengen functiescheidingseisen.

Het eerste type procesgang is mede afhankelijk van de kwaliteit van de processen (en dus de (autoritatieve bron) dataverzameling) bij de personeelsafdeling of HR organisatie (Let wel, in sommige organisaties wordt gebruik gemaakt van meerdere autoritatieve bronnen die door verschillende afdelingen beheerd worden, bijvoorbeeld voor extern personeel of (keten)partners). Hier ontstaat het signaal van in-, door- en uitstroom van personeel en de organisatorische informatie die kan worden overgenomen door het autorisatietoewijzings-proces. Hier ontstaat soms vertraging doordat managers eerder over het aangetrokken personeel willen beschikken dan de formele HR procedures zijn afgewikkeld (bijvoorbeeld door het uitvoeren van een Pre-Employment Screening – PES.) Een goede aansluiting met dit HR Proces is dan ook vereist.

Breng in het AM systeem drempelwaarden aan. Soms worden er wijzigingen aangebracht die tot veel wijzigingen in de rollen leiden. Bij bijv. meer dan 5% wijzigingen kan het systeem dan stoppen en een signaal afgeven.

AM-tooling, mits volledig gekoppeld aan het HR-systeem, is ook te gebruiken als bronsysteem voor personele informatie (de zogenaamde Yellow-pages), zeker als er meerdere bronnen gekoppeld zijn. Vaak is een interne website opgericht waarmee het personeel de eigen informatie kan aanpassen. Deze twee bronnen kunnen dan gecombineerd worden in het AM-systeem.

In de praktijk is het handig om voordat de formele HR ‘in-dienst-procedure’ is afgewikkeld het autorisatieproces te starten (het AM – systeem heeft dan nog geen formeel signaal gekregen). Een mogelijke oplossing is hier een koppelpunt tussen de HR administratie en het AM-systeem te modelleren. Het AM-systeem krijgt van het HR systeem tijdens het ‘in-dienst-proces’ een trigger, genereert een unieke identificatie van de medewerkers en geeft dat weer terug aan het HR systeem. Op basis van deze unieke identifier kan het autorisatieproces worden gestart (en vaak nog andere bestelprocessen). Dit moet overigens wel in lijn zijn met het beveiligingsbeleid. Soms mag een aankomend medewerker op een functie nog niet op de systemen voordat een expliciete goedkeuring van HR of veiligheidszaken (screening) rond is. Een expliciete waiver is dan een oplossingsmogelijkheid.

De bedrijfsprocessen in de business zijn de basis voor het begrijpen van de benodigde rechten en deze onderbrengen in het rollenmodel. Het inhoudelijk beheren van deze rollen is een decentrale aangelegenheid omdat in de business deze inhoud het best wordt begrepen. Stel met de business samen de namen op van de rollen, zodat die in die context helder zijn. Liefst wat meer rollen die duidelijk zijn dan streven naar een minimale set die tot onduidelijke formuleringen leidt. Het is belangrijk hier de balans te houden; een te groot aantal rollen leidt, zeker op termijn, tot onduidelijkheid en teveel beheerinspanning. De kaders daarvoor worden gesteld door de centrale beheerorganisatie. Deze ziet ook toe op het naleven van naamgevingsconventies, de discipline rond uitgifte van tijdelijke rechten en de kaders en borging van het decentraal uitgevoerde attestation-proces.

De beheerorganisatie zal ook betrokken moeten worden bij belangrijke veranderingen zoals cloud-computing en de verandering in het autorisatiemodel dat daarmee samenhangt.
Ook technische veranderingen in de applicaties zullen in de gaten moeten worden gehouden. Beheerorganisaties zijn vaak verdeeld in functioneel, technisch en applicatiebeheer (Model volgens Looijen, ook ITIL, ASL, BiSL) en mengvormen daarvan. Organisatorische veranderingen zijn niet standaard opgenomen in deze beheerorganisaties. Daar moet dus extra aandacht voor zijn.

Het centraliseren van dit beheer is een optie, dat hangt helemaal af van de grootte en complexiteit van de organisatie. In grotere complexe organisaties is het centrale beheer vaak ondergebracht bij de IT afdeling en worden de inhoudelijke rollen beheerd door de decentrale organisatie. Richt te allen tijde wel een aparte beheerorganisatie in met gespecialiseerde beheerders. De volwassenheid van de rollen moet passen bij de volwassenheid van de organisatie anders ontstaat verwarring. De AM-beheerders kunnen deze match in de gaten houden.

Samenvattend kennen de beheerfuncties de volgende gelaagdheid: Een centraal deel waarin de standaard en architectuur wordt bewaakt, een decentraal deel waarin de verbinding met de business wordt gemaakt en de lokale rollen worden beheerd. Het is belangrijk tijdens een project al meteen interne beheerders te laten meedoen om eventuele kennis van externe medewerkers over te nemen.

HIGHLIGHTS

- Aansluiting van het in-, door- en uitstroomproces met de HR processen is vereist.
- Scheiden van het aanvraagproces en het proces van inhoudelijk rollenbeheer
- Mogelijke KPI's: #rolaanpassingen; Doorlooptijd rolwijziging; #vragen over rolnamen; #rollen tegelijk in behandeling; #rollen per afdeling.

2.4. Psychologie van de medewerker

Over het algemeen zijn medewerkers bereid beperkingen in de toegewezen autorisaties te accepteren als dit het dagelijks werk niet belemmert of logisch is in de uitvoering van hun functie. Deze beperkingen moeten zijn beschreven in de uit te voeren bedrijfsprocessen en in het autorisatiebeleid waarin heldere functiescheidingscriteria zijn vastgelegd. Het communiceren van dit beleid en de uit te voeren taken zijn wezenlijk voor acceptatie door de gebruikers. Expliciet moet in een beveiligingsbeleid zijn terug te vinden of er gewerkt wordt met het "open tenzij" of "dicht tenzij" principe.
Tijdens het overdragen van het project aan de staande beheerorganisatie is de kennis vaak niet goed geborgd. Externen die bij het project zijn betrokken beschikken over waardevolle kennis die goed moet worden geborgd en overgedragen aan het interne personeel. Bij voorkeur wordt het project voor het grootste deel door interne medewerkers uitgevoerd zodat kennisdrain wordt vermeden.

Een ander fenomeen zijn de 'eilandjes' rond (legacy)systemen. Door eigenbouw autorisatieschil(len) is de kennis schaars en zijn standaard provisioning of reconcilliation[2] koppelingen niet mogelijk. Het autorisatiebeheer blijft in de eilandjes situatie achter bij het

[2] Reconcilliation is het vergelijken van de gewenste situatie met de werkelijke situatie.

volwassen beheer dat door het AM-project wordt opgeleverd, wat de kwaliteit van het totaal nadelig zal beïnvloeden. Uiteraard zijn business cases te maken voor het zodanig aanpassen van de legacy systemen dat automatische provisioning mogelijk wordt. Zorg er in ieder geval voor dat ook deze systemen, eventueel via handmatige werkorders uit het AM-systeem, worden aangesloten op de standaard procesgang.

Het nieuwe werken zal ook voor werknemers een andere houding ten aanzien van autorisaties en security verlangen. Het niet tijd- en plaats onafhankelijk werken zal behalve technische maatregelen ook een meer bewuste omgang van de medewerker verlangen. Het ene moment werk je op de laptop van het bedrijf, het andere moment op je eigen smartphone, je privé PC of op je tablet. Mogelijk neem je diensten af van een cloud provider en komen gegevens die je om snel te kunnen werken onbewust op plaatsen waar die niet thuis horen.
Een bewuste afweging door de werknemer voor het gebruik van al deze informatie is dan een vereiste. Zelfs als het gebruik van deze devices is toegestaan is voorzichtigheid geboden. Doordat gebruikers bewust met deze materie omgaan kunnen autorisaties worden aangepast aan de nieuwe steeds sneller wijzigende omstandigheden.

HIGHLIGHTS

- Zorg voor acceptatie bij gebruikers door duidelijke procedures afgestemd op de dagelijkse praktijk.
- Voorkom ‘eilandjes’ bij de inrichting van de beheerorganisatie. Neem alles mee.
- Voorkom het weglopen van expertise door van meet af aan eigen beheerpersoneel mee te laten doen met het project.
- Mogelijke KPI’s: #rollen specifiek voor mobiele toepassingen; #rollen voor legacy; #tijdelijke rollen; gemiddeld aantal transacties/permissies per rol.

16

INFORMATIE STRUCTUREN

3.1. Informatiearchitectuur

De informatiearchitectuur beschrijft de indeling in informatie attributen met de daarbij behorende standaardisatie en taxonomie. Hier worden de informatieobjecten gedefinieerd en geclassificeerd, waartoe toegang moet worden verleend middels autorisaties. In de architectuur wordt ook het autorisatie-/rollenmodel gedefinieerd. Dit rollenmodel is voor een belangrijk deel afhankelijk van de complexiteit van de informatievoorziening en de organisatie.

Het is zaak de AM-architectuur volledig te integreren in de informatiearchitectuur. Een succesfactor is het delen van de benodigde kennis bij de informatiemanagers en -analisten want vaak wordt het rollenmodel niet goed begrepen.

In een goed rollenmodel wordt in ieder geval de technische van de logische kant gescheiden. Dat verhoogt het begrip aan weerszijden en biedt goede mogelijkheden om het technisch en functioneel beheer in te richten.
Bij een complex IT-landschap kan gekozen worden voor meerlaags rollenmodellen. Die zijn wel complexer om te beheren, maak goede afwegingen bij deze keuze.

Eenmaal gekozen voor een rollenmodel is het zaak dat rollenmodel in de Enterprise Architectuur te verankeren om te waarborgen dat bij alle veranderingen in de organisatie het rollenmodel als belangrijke factor wordt meegenomen.

Bij Federated Identity Management is het van belang de daarvoor benodigde rollen apart, dus herkenbaar te benoemen. In de meeste gevallen zal toegang van deze externe partijen beperkt zijn tot enkele functies en bestanden. Definieer die vooraf in de informatie architectuur.

HIGHLIGHTS

- Zorg voor goede kennis van het autorisatie-/rollenmodel.
- Integreer het rollenmodel in de business- en informatiearchitectuur.
- Maak het werken onder architectuur verplicht in deze architectuur worden de piketpaaltjes geslagen over taxonomie, partitionering, toekomstige projecten ed..

3.2. Informatiebronnen

Het Access Management system wordt gevoed door bronnen zoals personeelsinformatie uit het HR systeem. De kwaliteit van deze brongegevens is van doorslaggevend belang voor het welslagen van een Access Management programma. Access Management gaat verder dan toegang verlenen voor het eigen personeel. Het systeem kan ook ingezet worden om de toegang op de systemen te verlenen van personeel van business partners of fusie partners of zelfs klanten (B2C). De autoritatieve bronnen bevinden zich dan buiten de invloedssfeer van het eigen bedrijf en er zullen afspraken moeten worden gemaakt over interfaces en informatiekwaliteit. Het faciliteren van meerdere autoritatieve bronnen heeft ook consequenties voor de unieke identificatie van personen; immers wat te doen met overlappende personeelsnummers en de koppeling van systemen die een beperking hebben ten aanzien van userid’s. Het verdient aanbeveling het AM-systeem een unieke identifier te

laten generen als basis voor de registratie. Dit unieke identificatiekenmerk (eng. Unique-identifier) zal dan wel opgenomen moeten worden in de gekoppelde HR systemen. In de praktijk blijkt dit redelijk eenvoudig gerealiseerd te kunnen worden.

HIGHLIGHTS

- Hou van begin af aan rekening met meerdere autoritatieve bronnen ten aanzien van personele informatie.
- De kwaliteit van de brongegevens moet op het voor een succesvolle AM-implementatie vereiste niveau worden gebracht.
- Zorg voor een ontkoppeling van de bronsystemen en het AM-systeem.
- Vervuiling in het bronsysteem dient door de eigenaar van de bron te worden opgelost. (Deze activiteit valt niet noodzakelijkerwijs binnen het project/traject)
- Mogelijke KPI's: #autoritatieve bronnen; #exceptionele aanvragen (dit zijn aanvragen veroorzaakt door foutieve brongegevens)

3.3. Rapportages

Rapportages uit AM-systemen voor auditdoeleinden (soll-ist controles) zijn de meest tot de verbeelding sprekende output, maar ook de uitwisseling van provisioning gegevens met de uitvoerders daarvan (provisioning systemen, oplosgroepen, platformbeheerders, service desk medewerkers) is output die kwalitatief aan goed normen moet voldoen. Rapportages volgen vaak de drie niveaus strategisch, tactisch en operationele rapportages. Belangrijk voor de acceptatie is dat de rapportages voor het directe personeel begrijpelijk, inzichtelijk, correct en leesbaar is in een formaat dat is toegesneden op de doelgroep. Het scheiden van de technische benaming van de rollen van de functionele benaming of de benaming die is afgeleid van de activiteiten in een bedrijfsproces is daarbij een must.

Zorg ervoor dat functiescheiding blijkt uit de rollenbenaming zodat het voor iedereen duidelijk is welke rollen er wel of niet samengevoegd kunnen worden.
Soll-Ist rapportages zijn voor de auditors het meest belangrijk, het systeem kan de zaken enorm versimpelen door geautomatiseerde Soll-Ist rapportages te maken waarbij de verschillen meteen inzichtelijk zijn voor de controleur.
Een andere vorm van rapportage is het inzicht in de performance van de aanvraagprocedures. De snelheid van het verwerken van aanvragen kan worden gemeten en gerapporteerd. Aanvragen en de behandeling daarvan kunnen beschouwd worden als een logistiek proces, het is handig voor de aanvragers en beheerders om dit proces inzichtelijk te maken met specialistische rapportages. (vb. in welke processtap de aanvraag zich bevindt)

HIGHLIGHTS

- Zorg ervoor dat rapportages aansluiten bij de doelgroep.
- Automatiseer repeterende taken zoveel mogelijk zoals Soll-Ist controles.
- Mogelijke KPI's: #soll-ist rapportages; #fouten in soll-ist; gemiddeld aantal regels in soll-ist vergelijkingen; #verschillende rapportages; #personen waaraan een specifieke rol is toegekend; #foutief afgehandelde aanvragen; #ingetrokken rollen; Aantal keer dat een uitzonderingsprocedure is gebruikt.

3.4. Informatie regels

Rol gebaseerd autoriseren sluit het voldoen aan vooraf gestelde regels (rules) niet uit. Het is aan te bevelen om enkele regels te stellen waaraan rollen moeten voldoen. Zoals speciale

rollen (superuser rechten) of rechten tot hoog vertrouwelijke gegevens. Deze regels kunnen dan worden opgenomen in ontwerpvoorwaarden en aansluitvoorwaarden. Classificatieschema's kunnen ook worden beschouwd als regels waaraan informatie moet voldoen zodat de rechten op deze informatie-elementen kunnen worden toegekend op basis van bijvoorbeeld vertrouwelijkheid. Denk hierbij aan regels ten aanzien van de omgang met klantinformatie en informatie van VIP's. Dit zijn vaak bijzondere gegevens waarvoor aparte autorisatiegroepen worden gemaakt.

Tijdelijke autorisaties worden vaak permanente autorisaties. De huidige AM-pakketten voorzien in het definiëren van een verloopdatum. Maak daar gebruik van. Bij het aanvragen van tijdelijke autorisaties kunnen bestaande functiescheidingsregels worden overtreden, maak dat een bewuste keuze. Het is in het algemeen de verantwoordelijke die hier in staat gesteld moet worden zijn / haar verantwoordelijkheid te nemen, door expliciet daar de beslissing neer te leggen en de manager te voorzien van de rapportages en signalen om dat te ondersteunen.

De hoogste mate van volwassenheid wordt hier bereikt door de voorspelbaarheid van de afhandeling van de autorisatieaanvragen. De autorisatieaanvragen zijn volledig gebaseerd op van bedrijfsprocessen afgeleide rollen, met heldere functiescheidingsregels waardoor het AM-systeem al bij het aanvragen functiescheidingsconflicten opmerkt. Tegelijk zijn de autorisatieaanvragen altijd gebaseerd op een in- door- of uitstroom gebeurtenis of een wijziging van de bedrijfsprocessen of een wijziging in de gebruikte business processen of applicaties. Echter deze wijzigingen zijn altijd het gevolg van een kwalitatief goed wijzigingsproces.

Het is ook aan te bevelen af en toe te controleren of er rollen of autorisaties zijn gedefinieerd waar gedurende langere tijd geen gebruik van is gemaakt. Samen met de eigenaar van de rol of autorisatie kan dan worden besloten deze 'zwevende' rol / autorisatie te verwijderen.

HIGHLIGHTS

- Zorg voor een goede classificatie van (beveiligings/autorisatie) regels.
- Zorg voor regels voor speciale rollen.
- Zorg voor regels voor hoog vertrouwelijke gegevens.
- Mogelijke KPI's: #dode rollen; specificatie van dode rollen; #rollen afgekeurd.

3.5. Informatie kosten

De kosten van AM-projecten zijn niet altijd goed voorspelbaar. De basisinrichting is veelal wel goed in te schatten, maar vertragingen doordat de basisinformatie kwalitatief moet worden verrijkt is vaak niet goed in te schatten waardoor het project kan uitlopen in tijd en kosten. Hierover is in expertbrief 3 al het een en ander geschetst. In de praktijk is het handig om tijdens de voorstudie zoveel mogelijk risico's in kaart te brengen en deze te kwantificeren. Het blijkt dat het opleiden van beheerders en het inrichten van de beheerorganisatie meer kosten met zich meebrengt dan oorspronkelijk is begroot. Wijzigingen tijdens het project zijn vaak de oorzaak van kostenverschuivingen.

Het snel onderbrengen van project activiteiten in de lijnorganisatie is, afhankelijk van de volwassenheid van de lijnorganisatie aan te bevelen, dit kan uiteindelijk een reductie teweegbrengen in de projectkosten. Maar de totale kosten zullen hierdoor niet relevant

worden beïnvloedt.

Omdat AM-projecten worden gekenmerkt door een lange doorlooptijd is het van belang (kleine) successen te vieren en kleine overzichtelijke uitbreidingen te definiëren.

HIGHLIGHTS

- Zorg voor voldoende opleidingsbudget voor beheerders.
- Breng zo snel mogelijk project activiteiten onder bij de lijnorganisatie.
- Biedt weerstand tegen projectkosten reductie tijdens het lopende project.
- Een andere mogelijkheid is incentives te genereren door het verminderen van licentiekosten doordat een beter beheer van rollen tot verminderde behoefte van licenties leidt (ook omdat aanvragen snel en voorspelbaar verlopen worden licenties als zij niet meer nodig zijn snel ingeleverd.).
- Mogelijke KPI's: #rollen met licentie (en, zo mogelijk, de kosten daarvan); € opleidingsbudget.

20

SERVICES EN TOOLING

4.1. Welke AM-services zijn gerealiseerd en welke zijn gewenst? Intern en extern (federatief)

Het kiezen van passende tooling is een delicaat proces van afwegen van requirements, de geboden functionaliteit en de toekomstvisie. Complexe systemen zoals ERP systemen zijn niet meer te beheersen zonder goede tooling. Daar zou het vanzelfsprekend moeten zijn goede tooling in te zetten. Als men een minder complex IT landschap heeft, zijn eenvoudige tools vaak de beste keuze. Deze tooling kent weinig extra functionaliteit wat ervoor zorgt dat er geen complexe implementaties kunnen ontstaan. Er is een duidelijk verschil tussen tools die uitsluitend Access management functionaliteit bieden en tooling die tevens de in-, door- en uitstroom processen kunnen faciliteren. Combinaties zijn ook op de markt verkrijgbaar inclusief tools met uitgebreide provisioning capaciteiten. Deze capaciteiten zijn echter altijd gebaseerd op marktstandaarden. Provisioning naar maatwerksystemen is per definitie lastig. Stelt men de vraag in welke omgeving het AM-systeem het beste kan worden gezien, dan is er één voorwaarde om te kunnen doorgroeien naar een volwassen AM-inrichting en dat is de combinatie met een SIEM (Security Incident en Event Monitoring) omgeving. Dit kan bijvoorbeeld gefocust zijn op het traceren van activiteiten van beheerders met hoge rechten (audittrail), het kunnen blokkeren van activiteiten of gegevensverzamelingen.

Opsomming van serves is al in expertbrief 2 (architectuur) behandeld.

HIGHLIGHTS

- Ondersteuning van Open protocollen zoals SAML, SCIM en/of SPML zijn aan te bevelen.

4.2. Software

Volledige pakket oplossingen voor Access- en Identity management zijn schaars. Binnen de grotere organisaties bieden de standaardpakketten onvolledige functionaliteit inzake werkstroom, provisioning, functiescheiding definities, ondersteuning van rule en role based modellen en de omgang met superuser rechten. Hierdoor is aanvullend maatwerk vereist wat het initiële project alsmede het onderhoud duurder maakt.

Het verdient aanbeveling de complexiteit van het te kiezen pakket te laten aansluiten bij de grootte en complexiteit van de organisatie en het te beheren IT-landschap en informatiesystemen. Het uitvoeren van een pilot met vastgestelde criteria en voorlichting van de fabrikant zijn voor een dergelijk project onontbeerlijk.

Complexe pakketten kunnen meer maar zijn ook lastiger te beheren wat hogere exploitatielasten met zich meebrengt.

HIGHLIGHTS

- Kies een pakket dat past bij de organisatie en complexiteit van het IT-landschap.
- Beperking van functionaliteit kan goed zijn omdat het de mogelijkheden tot maatwerk sterk beperkt.
- Selecteer ‘proven’ technology, toegesneden op de business eisen.

- Staar je niet blind op requirements, in de huidige pakketten zit veel kennis die uiteindelijk tot betere implementaties leiden.

4.3. Hardware & omgevingen (ontwikkel, test, acceptatie en productie OTAP)

Het beperken van autorisaties tot autorisaties in productiesystemen is in eerste aanleg een goede keuze om te starten. Autorisaties in acceptatie zouden echter gelijk moeten zijn aan de productieomgeving. Vele fouten komen voort uit het incorrect inrichten van de autorisaties. Streven naar volledigheid in de OTAP straat is dan ook aan te bevelen op de langere termijn. Waarbij de TAP omgevingen zoveel mogelijk identiek moeten zijn, aan de O-omgeving worden minder eisen gesteld.

Hoewel in ontwikkelomgevingen geen streng autorisatieregime hoeft te gelden, (dat zou contraproductief werken) is in-, uit- en doorstroom van personeel wel belangrijk. Denk hierbij aan rechten waarbij het mogelijk is software door te zetten van ontwikkel naar overige omgevingen. Het AM-systeem zelf zal ook ontwikkeld of geconfigureerd moeten worden, daar gelden in principe geen andere regels.

In de praktijk blijkt dat als autorisatiebeheer een volwassen plaats inneemt in het bouwproces, het aantal fouten in productie dat te wijten is aan verkeerde autorisaties verminderd. Tevens worden de autorisatiemogelijkheden in het bouwproces zo ingericht dat dit tot betere en voor de buitenwereld meer logische oplossingen leidt.

Wordt dit tegen een volwassenheidsmodel aangehouden dan is integratie van het autorisatie-requirements in het bouwproces de beste garantie voor een volwassen AM.

HIGHLIGHTS

- Focus op productiesystemen in aanvang.
- Denk aan het beheer van speciale bevoegdheden.

4.4. Project of zelfbouw tooling

In het algemeen zullen pakketten de voorkeur genieten boven zelfbouw, het is in vele gevallen goedkoper, de pakketten zijn beter gedocumenteerd en bieden best-practices waar veel ervaringen uit de praktijk in zijn verwerkt.

Toch is in enkele gevallen zelfbouw zeker een optie daar waar standaard pakketten ontoereikende functionaliteit bieden en er veel access management van eigengemaakte bedrijfssoftware moet worden gemanaged is de overweging voor zelfbouw zeker gerechtvaardigd.
Uit de praktijk blijkt dat de standaard pakketten toch minder functionaliteit bieden dan noodzakelijk is voor een goed autorisatiebeheer. Daarom zijn bij grote bedrijven de meeste implementaties van standaardpakketten hybride oplossingen met zowel het standaardpakket als maatwerk.

Als we dit afzetten tegen een maturity-level dan zijn er slechts heel weinig standaardpakketten die alle functionaliteit bieden om het hoogste niveau van volwassenheid te ondersteunen in complexe omgevingen. In redelijk overzichtelijke IT-omgevingen is dat zeer wel haalbaar.

22

In een standaardpakket situatie wordt men wel sneller gedwongen een heldere keuze te maken en dat zal de snelheid waarmee men naar een volwassen AM-omgeving toe groeit wel vergroten. Men is immers minder geneigd via maatwerk een oplossing te maken voor een proces of procedure die goed beschouwd niet een structurele verbetering inhoudt.

HIGHLIGHTS

- Zorg bij maatwerk voor structurele verbeteringen, blijf niet in oude gewoonten hangen.

INFRASTRUCTUUR

5.1.Hoe ziet de infrastructuur er uit?

De Centrale Directory wordt in het ondersteunen van de moderne architecturen belangrijker. Daarnaast vindt er een verschuiving plaats waarin de Identity Store van de Autorisatiesystemen de centrale plek wordt van opslag van personeelsgegevens. Dat vormt dan weer de basis om ook niet in HR administratie opgenomen personeel te kunnen ondersteunen zoals Federated Identity Management (FIM) vereist.
Interessant hierbij is wie dan de eigenaar is van deze en daaraan gelinkte administraties.
Overige infrastructurele aspecten zijn de inrichting van de directory structuur (met name hoe applicaties daarmee om moeten gaan, dat is vaak ondoordacht en daarmee qua autorisaties lastig te onderhouden), de overstap naar SharePoint[3] structuren, het kunnen onderscheiden van 'eigen' directories moet allemaal ondersteund kunnen worden door de infrastructuur.

De legacy access management systemen zijn vaak niet goed integreerbaar in een moderne AM-opzet, ondersteunen geen rollen of autorisatieprofielen. Vraag is of dit in een moderne AM-oplossing zodanig kan worden gemodelleerd dat een moderne werkwijze toch wordt ondersteund.

Dwing af dat alles door de OTAP straat gaat. Access management omgevingen zijn complexer te beheren dan andere omgevingen.
In principe is een AM-systeem niet bedrijfskritisch, het uitvallen van een AM-systeem mag niet leiden tot het niet kunnen werken in de business. Zorg dus voor alternatieve, handmatige processen.

HIGHLIGHTS

- Centrale directory-services worden belangrijker in moderne AM-systemen.
- Identity store van AM-systeem wordt uitvoerende instantie voor ontsluiten van HR systemen.
- Legacy access management systemen zijn vaak niet goed integreerbaar in een moderne AM-opzet.
- Maak het AM-team verantwoordelijk voor begeleiding van de projecten en laat deze veranderingen inbedden in de infrastructuur.

5.2. Worden standaard protocollen gebruikt?

Standaard open protocollen zijn van de laatste tijd. In veel gevallen zullen er nog legacy producten en aanverwante protocollen gebruikt worden. In veel grote bedrijven wordt gewerkt met een vorm van een Enterprise Service Bus (ESB). Een dergelijke centrale bus helpt om standaard manieren van communicatie te ondersteunen. In veel gevallen zal er ook gebruik gemaakt worden van koppelingen met helpdesk systemen om de werkorders die per platform worden gegenereerd te versturen. De werkorders worden vervolgens (handmatig) door de platformbeheerders uitgevoerd. In sommige AM-systemen worden de werkorders centraal neergezet en is communicatie niet vereist.

[3] SharePoint is een product van Microsoft ™

Hier kan een link gelegd worden met de volwassenheid. De ideale wereld bestaat uit allemaal koppelingen gebaseerd op open protocollen. Alle systemen worden geautomatiseerd geprovisioned en Soll-Ist controles worden uitgevoerd met behulp van deze koppelingen. Omwegen rond deze autorisatievoorziening zijn niet aanwezig, vanwege de snelheid van het verwerken van autorisatieaanvragen is er ook geen behoefte eromheen te gaan. Dit is het hoogst haalbare volwassenheidsniveau.

Zodra werkorder koppelingen of handmatige koppelingen worden ingezet hoeft het volwassenheidsniveau niet sterk te dalen, het kunnen nog steeds correcte voorspelbare koppelingen zijn, als een klein deel van de systemen waar weinig dynamiek is te verwachten daarmee is gekoppeld is het volwassenheidsniveau nog alleszins hoog.

Daarna volgt de hybride fase waarin de koppelingen niet standaard zijn, op legacy gebaseerd, de koppelingen ook niet volledig zijn (niet alle gewenste functionaliteit kan met de koppeling worden gerealiseerd) en de dynamiek van deze legacy omgeving is ook nog hoog. Dit levert een beduidend lager volwassenheidsniveau. De garanties die kunnen worden afgegeven over een correct autorisatiebeheer zijn beperkt.

Voor het aanhaken op de cloud diensten zijn er verschillende protocollen populair aan het worden zoals SCIM (Simple Cloud Identity Management). Populairder dan SPML dat door de cloud community te zwaar en te gecompliceerd wordt gevonden.

HIGHLIGHTS

- Een volledig op open – autorisatieprotocollen gebaseerd AM levert het hoogst haalbare volwassenheidsniveau.

CONCLUSIES EN VERVOLG

Het invoeren van een AM-systeem blijkt in de praktijk lastig te zijn zeker ook omdat het een onderwerp is dat meestal niet hoog op de agenda van de directie staat. Toch blijkt dat alle bedrijven die zich deze moeite hebben getroost er zeer tevreden over te zijn, niet in de laatste plaats omdat de eigen bedrijfsprocessen daardoor beter gestructureerd en van hogere kwaliteit geworden zijn.

Onder meer uitbesteding van bedrijfstaken aan andere meer gespecialiseerde bedrijven zorgt voor toenemende noodzaak voor het meer federatief inrichten van access management. Een andere driver voor Federated identity management zijn de Cloud computing en BYOD ontwikkelingen.

Al deze mogelijkheden zijn op een volwassen wijze te ontsluiten als de basis inrichting van access management op orde is.

Een logische conclusie is dat een volwassen access management voor bedrijven onontbeerlijk is geworden. Er is veel ervaring opgedaan in de industrie zodat de kans op een geslaagd AM project beduidend is toegenomen.

Federated Identity Management is de volgende stap die bedrijven al aan het nemen zijn en in toenemende mate zullen gaan nemen.

26

LITERATUURLIJST

De expertgroep beveelt ter aanvulling of ter verdieping van de behandelde onderwerpen de volgende literatuur aan:

- Expertbrief "Access management deel1:Visie", zie https://www.pvib.nl/expertbrief
- Expertbrief "Access management deel2:Architectuur", zie https://www.pvib.nl/expertbrief
- Expertbrief "security architectuur", Jaargang 2, nr4, december 2006, zie https://www.pvib.nl/?page=6259972
- Expertbrief "Access management deel3:Project management".
- PI-RBAC_v_1_0a[1].pdf http://www.pvib.nl
- NIST reeks http://csrc.nist.gov/
- SOGP 2007 (www.securityforum.org)[4]
- OSA, open security architecture http://www.opensecurity.org
- Enterprise Access Management http://www.JPVincent.nl/BIAMEIA
- ISO 27001 & ISO 27002

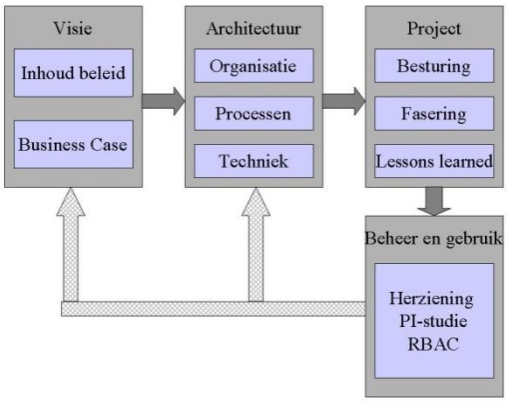
Artikelen:

- Business Oriënted Authorization Model (jaargang 2010,nummer 2) https://www.pvib.nl/download/?id=17670567&download=1
- ABAC https://www.pvib.nl/download/?id=6474160&download=1
- ABAC https://www.pvib.nl/download/?id=6474183&download=1
- CBAC https://www.pvib.nl/download/?id=10511450&download=1
- Diverse artikelen over protocollen (SAML, SPML, SCIM) bron Wikipedia.

[4] SOGP 2011 is ook al uit maar niet publiek beschikbaar.

BIJLAGE 1. SESSIE-OVERZICHT EXPERTBRIEVEN ACCESS MANAGEMENT

Aanpak
De voorbereidingsgroep wil producten opleveren van een hoog kwaliteitsgehalte binnen een reëel tijdsbestek en heeft daarom het onderwerp access management in vier hoofdgebieden opgesplitst (zie figuur 1). Deze hoofgebieden worden in gescheiden sessies besproken en vallen samen met de stappen die doorlopen moeten worden wanneer men met access management aan de slag wil gaan. Per hoofdonderwerp wordt een expertbrief opgeleverd. Iedere expertbrief kan in principe resulteren in aanvullende themasessies, vervolgartikelen en handreikingen, afhankelijk van de belangstelling en het animo onder deskundigen om hierin te participeren.



Figuur 1.1 Opsplitsing van onderwerp access management in 4 expertbrieven.

De vier hoofdgebieden behelzen het volgende:

1) Visie: Het eerste onderdeel betreft het vormen van een visie over het daadwerkelijk bestaan van één ideaal access management concept. Start een ideaal concept met het hebben van concreet beleid en wat die moet die beschrijven? Het realiseren/implementeren van een compleet access management-concept zal, als gevolg van kosten (businesscase) of complexiteit, niet altijd volledig of in één keer haalbaar zijn. Welke risico's worden onderkent die het succes van een implementatieproject kunnen tegenwerken.

2) Architectuur (deze expertbrief): In het tweede onderdeel wordt access management vanuit architectuur beschreven. Zowel contextueel, als de aspecten omtrent organisatie- en procesinrichting, autorisatiemodellering en techniek.

3) Projectmanagement: In het derde onderdeel zal worden beschreven hoe de implementatie kan worden gerealiseerd en welke werkwijzen en projectinrichtingen daarbij kunnen worden toegepast.

4) Beheer en gebruik: Het vierde onderdeel richt zich op de operationele situatie. Het beantwoord de vraag hoe een beheerorganisatie er concreet uit kan zien, welke ervaringen zijn opgedaan met beschikbare hulpmiddelen, etc. Ook kan, als gevolg de activiteiten van de expertgroepen, de visie op access management zodanig zijn ontwikkeld dat dit een bijdrage kan leveren aan de aanpassing van de PI-studie RBAC.

BIJLAGE 2. INFORMATIE OVER DE DEELNEMERS

Onderstaande deelnemers hebben bijgedragen aan deze expertbrief. Mocht u met een van hen contact willen opnemen dan kan dat via het secretariaat van het PvIB, zie http://www.pvib.nl/contact.

Jean-Pierre Vincent

Vervult rollen als adviseur, projectmanager, architect en consultant in complexe identity & access management-programma's bij de overheid en grote instellingen in de financiële, telecommunicatie en industriële branche.

Peter Hoogendoorn

Peter is als security manager betrokken bij een IDM project in de financiële sector en is als consultant, architect en auditor werkzaam geweest in de overheids- en financiële sector.

Karin van de Kerkhof

Karin heeft als consultant ervaring met identity&access management projecten in de overheids- en financiële sector. Is verder werkzaam als audittor.

Jan-Roel Löwenthal

Jan-Roel is voornamelijk werkzaam in de overheidssector. Houdt zich bezig met Servicemanagement, Architectuur en Informatiebeveiliging. Is bij zijn werkgever focus arealeader van de community identity & access management en heeft op dat vakgebied bij verschillende klanten ervaring opgedaan.

Karel van Oort

Karel is als security consultant betrokken geweest bij verscheidene identity en access management projecten.

Piet Kalverda

Piet is als security consultant werkzaam in de financiële sector en is betrokken bij de implementatie identity en access management.

Wiyaykumar Jharap

Wiyaykumar houdt zich als consultant en projectmanager bezig met Security Governance, Risk & Compliance en IAM. Op het gebied van IAM is hij betrokken bij IAM-implementaties in de industriële en semi-overheidssector.

Peter Lucas

Peter is Servicemanager en identity en access management en geeft leiding aan een team serviceconsultants. Hij is tevens verantwoordelijk voor de totstandkoming van IAM-servicecontracten voor verscheidene klanten.

John van Westeneng

Is als IAM consultant, architect en projectmanager werkzaam in verscheidene identity en access management projecten in Nederland en België.

Renato Kuiper

Renato is management consultant en richt zich op het snijvlak van informatiebeveiliging, risicomanagement en architectuur. Vanuit die invalshoeken heeft hij veel ervaring opgedaan in Identity en Access Management projecten.

Aaldert Hofman

Werkt sinds 1995 op het vakgebied van informatiebeveiliging en architectuur. In uiteenlopende rollen van architect tot projectmanager heeft hij ervaring opgedaan in identity en access management projecten, met name bij financiële instellingen. Hij heeft meerdere artikelen op dit gebied geschreven en is jaren lid geweest van de redactieraad van Informatiebeveiliging.

Bert van Ingen

Is sinds eind jaren 80 werkzaam in de ICT, oorspronkelijk in de technische automatisering, daarna in kantoorautomatisering en netwerkbeheer. Als IT- en Security manager binnen grote zakelijke en financiële dienstverleners ruim 10 jaar verantwoordelijk voor uitvoering en beleid van continuïteit, informatiebeheer en –beveiliging.

Jaap Scheepstra

Is als architect betrokken bij projecten omtrent smartcards en identity en access management o.a. in de financiële sector.

30

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit:

WORDT LID VAN HET PVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN…

Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en IT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

https://www.pvib.nl/abonnementsinformatie