PvIB Expertbrief – Oktober 2009
ISSN 1872-4876, jaargang 5 – Nr. 2

Access management (Deel 1: Visie)

Jean-Pierre Vincent

Mike Chung

Aaldert Hofman

Bert van Ingen

Wiyaykumar Jharap

Piet Kalverda

Karin van de Kerkhof

Leon Kuunders

Jan-Roel Löwenthal

Henk Marsman

Damiën Meijer

Tonne Mulder

Karel van Oort

Jaap Scheepstra

Door strengere wet- en regelgeving, het steeds meer digitaliseren van informatie en het automatiseren van werkprocessen, groeit de aandacht voor access management. Veel bedrijven en instellingen onderzoeken hoe het professioneel en eventueel het centraal inrichten van access management, hieraan een bijdrage kan leveren. Andere redenen voor de toenemende aandacht zijn: het oplossen van auditbevindingen, het verbeteren van het serviceniveau m.b.t. het aanvragen en intrekken van autorisaties en het naar beneden brengen van de beheerkosten hiervan.
Deze expertgroep buigt zich in 4 sessies over access managementvraagstukken zowel vanuit lijn- als project situaties. Deze Expertbrief richt zich op beleid, project risico's en kosten/batenaspecten.

Pagina

2 INLEIDING EN SITUATIESCHETS

Aanleiding

Steeds meer bedrijven buigen zich over identity- en access managementvraagstukken. Deze vraagstukken zijn in essentie vaak dezelfde, alleen verschillen de bedrijfssituaties en daardoor de oplossingsrichtingen. Om te voorkomen dat wielen opnieuw worden uitgevonden, worden deze vraagstukken door experts geformuleerd en worden aanpak- en oplossingsrichtingen uitgewerkt in 4 expertbrieven, waar deze er een van is. Hierdoor kan de kennis op effectieve wijze worden hergebruikt.

Aanpak

Access management is complex. 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 het onderwerp ‘access management visie’.

Scope

De scope van deze expertbrief richt zich op access management. 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 geen aandacht wordt besteed aan identificatie- en authenticatie-oplossingen, beheer en controle op smart-cardoplossingen, Single-Sing-On (SSO) oplossingen en mechanismes om te controleren of ‘je bent wie je zegt dat je bent’, is buiten de scope. In deze expertbrief gaat de aandacht uit naar wat nodig is voor het verstrekken van autorisaties: beleid, organisatiestructuur, processen, bemensing, administratie en middelen.

Doelstelling

Deze expertbrief heeft tot doel een hulpmiddel te zijn bij het implementeren of verbeteren van een access management-organisatiestructuur en beheeromgeving. 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 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* 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* 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.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

Toelichting op access management:
Access management betreft het regelen van de toegang van een resource tot data of het mogen gebruiken van een service. In beide gevallen moet worden vastgesteld of de betreffende resource het recht heeft om bij de databron te komen (de resource mag de data inzien of muteren) of de service te gebruiken (bijvoorbeeld: licentie is voor de resource beschikbaar). In een enterprise-omgeving gaat het hierbij om veel rechtenverstrekkingen en de controle daarop (schaalgrote). Daarom loont het zich om de uitvoering daarvan efficiënt in te richten middels helder beleid, strakke processen, juiste bemensing, correcte administraties en goede hulpmiddelen.

Totstandkoming expertbrief
Deze publicatie is het resultaat van de 1e 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 zijn als volgt ingevuld:

Probleemeigenaar:	Karin van de Kerkhof
Facilitator:	Tonne Mulder
Co Facilitator:	Jan-Roel Löwenthal
Ghostwriter:	Jean-Pierre Vincent

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

4

DE ONDERZOEKSVRAGEN

Vragen die tijdens de workshop zijn geformuleerd: Bestaat er een ideaal access management concept (AM-concept)? Welke kosten/baten worden onderkend? Wat levert het wel en niet op?

De studie Role Based Access Control versie 1.0 van het Platform Informatiebeveiliging beschrijft waar een 'goed ingerichte' access management -organisatie aan moet voldoen. Het kan derhalve dienen als kader voor het voorlopige 'ideaal plaatje' voor het AM-concept (punt 4 in figuur 1). Door dit ideaal plaatje te leggen naast de beleidseisen en prioriteiten, kan voor een organisatie de ideale oplossing worden bepaald (punt 3 in figuur 1). Wanneer bijvoorbeeld 'optimale security' als hoofddoel is gesteld, dan leidt dat tot een andere ideaaloplossing dan waneer de hoofddoelstelling is het omlaag brengen van de beheerkosten. De vraag daarbij is wat het beleid moet beschrijven om volledig te zijn.

Businesscase-aspecten als 'wat levert het me op' zijn vaak moeilijk in cijfers uit te drukken. Hoe stellen we nu vast wat goed ingericht access management oplevert? Andere vragen zijn: hoeveel indirecte kosten worden bespaard en waar bestaan die eigenlijk uit, welke directe kostenbesparingen gaat het me opleveren, hoeveel bedragen de eenmalige investeringskosten voor beheer, hoeveel bedragen de implementatiekosten, wordt zicht en grip verkregen op de uitgegeven autorisaties, operationele beheerkosten, etc?

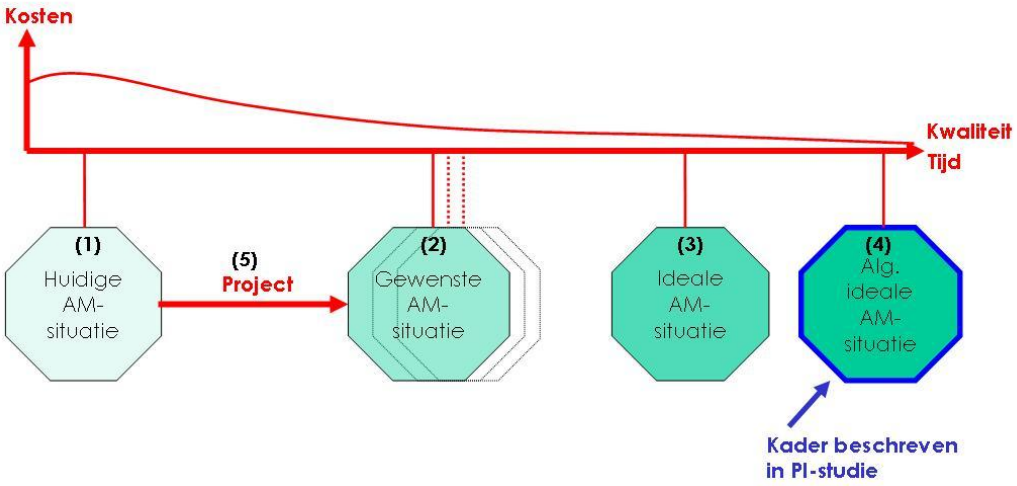


Fig. 1. Hoe kan vorm worden gegeven aan de in de PI-studie beschreven doelstellingen?

Samenvattend zijn de vragen:

1. Bestaat er een ideaal access management concept?
2. Welke elementen dienen er in het beleid te worden afgedekt?
3. Wat zijn de primaire drivers voor AM (benefits in de business case)?

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

BESTAAT ER EEN IDEAAL CONCEPT?

Over de vraag of er één ideaal access management concept is, zijn de sessie-leden het over het algemeen eens dat altijd dezelfde elementen (vraagstukken) spelen bij een in te richten of te optimaliseren lijnorganisatie. Deze elementen zijn:

- helder beleid;
- centrale gecoördineerde autorisatiebeheer- en controleprocessen;
- een (deels) centrale organisatie met helder beschreven taken & verantwoordelijkheden;
- een centraal beheerde of gecoördineerde administratie;
- een centraal tool ter ondersteuning van de processen (workflow) en administratie.

De invulling en diepgang van deze elementen kan per bedrijfssituatie verschillen. Deze is volledig afhankelijk van het huidige en het nagestreefde volwassenheidsniveau van de organisatie. Omgekeerd zouden wel verschillende volwassenheidsniveaus van organisaties kunnen worden gedefinieerd, waarin per niveau is aangegeven aan welke vraagstukken van access management invulling moet zijn gegeven. Zo kunnen organisaties doelgericht en stapsgewijs hun access management situatie verbeteren. Het beschikken over een ideale access management situatie is voor organisaties immers geen doel op zich.

Het is daarom niet mogelijk om één ideaal concept te beschrijven. Wel kan een concept worden opgedeeld in componenten. Per component is de funtionaliteitswens en oplossingsrichting redelijk dezelfde. De oplossingsrichting kan conceptueel redelijk uniform worden beschreven, maar blijft dan nogal abstract en weinig concreet.

Er is niet één invulling voor het ondersteunen van de abstracte funtionaliteitswens en oplossingsrichting. Logisch gezien lopen concrete oplossingen sterk uiteen.

Het is derhalve beter te stellen dat het goed mogelijk is een optimaal en universeel referentieconcept te beschrijven, die per vraagstuk informatie aanreikt en ondersteund bij het maken van de juiste afwegingen per component.

Deze, de overige drie geplande access management expertbrieven en de PI-studie zijn derhalve bedoelt als referentieconcepten voor access management.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

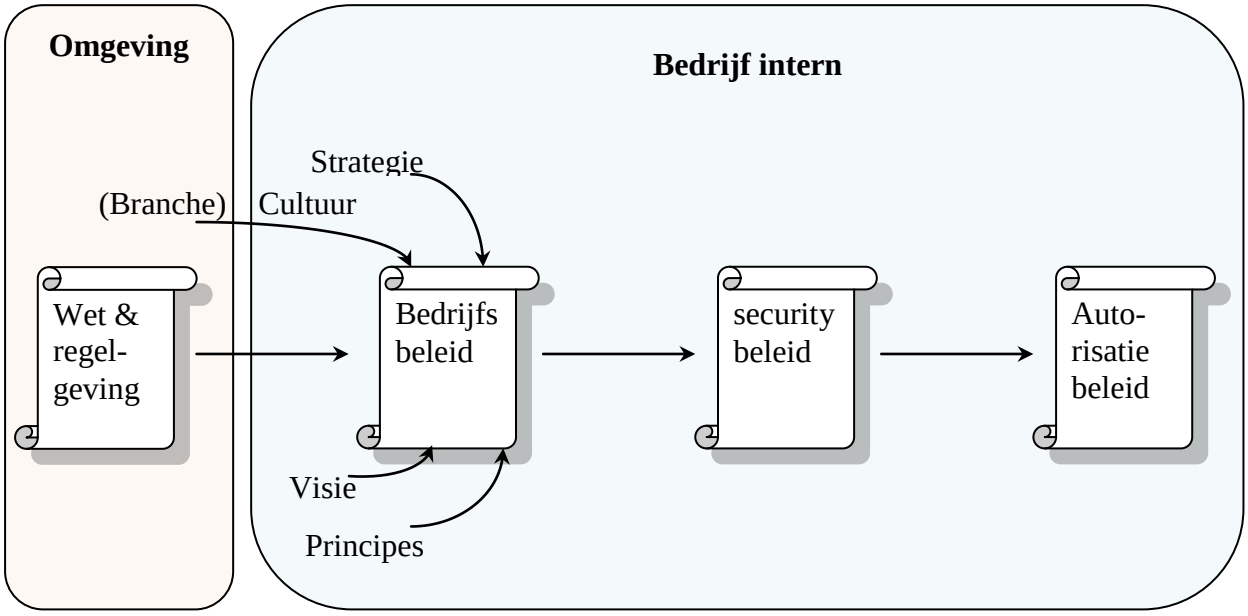
6 AUTORISATIEBELEID

Of het access management in een organisatie voor verbetering in aanmerking komt, kan alleen worden vastgesteld als het bedrijfsbeleid daar doelstellingen in nastreeft. Deze doelstellingen, soms deels in abstracte vorm opgelegd door de omgeving van de organisatie (bijvoorbeeld door wet& regelgeving), zijn niet altijd helder geformuleerd.

Een organisatie formuleert beleid om de te hanteren principes te beschrijven en kenbaar te maken. Op het beleid zijn factoren van invloed als wet en regelgeving, maar ook cultuur, visie, principes, strategie, etc.. Bedrijfsbeleid moet aangeven wat het volwassenheidsniveau is dat men nastreeft en hoe men dit nastreeft. Een van de aandachtsgebieden daarbinnen is security. Autorisatiebeleid zou deel moeten uit maken van het geformuleerde securitybeleid.

Dit hoofdstuk beschrijft vraagstukken die moeten kunnen worden beantwoord in autorisatiebeleid.

Een overzicht van deze beleidsstructuur is weergegeven in figuur 1.



Figuur 1. Beleidsstructuuroverzicht.

Autorisatiebeleid moet helder beschrijven aan welke criteria de autorisatiebeheerorganisatie moet voldoen en welke criteria dienen te worden gehanteerd voor beheren van autorisaties. Deze criteria richten zich onder andere op de werkwijze voor het vaststellen, verstrekken en controleren van autorisaties. In onderstaande tabel zijn aandachtspunten en richtlijnen beschreven.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

Aandachtspunten voor autorisatiebeleid:

<table>
<tr><th>Nr</th><th>Omschrijving</th></tr>
<tr><td>AB1</td><td>Beleid moet aangeven welke taken en verantwoordelijkheden aan ‘eigenaren’ zijn toebedeeld en hoe wordt gemeten dat zij daaraan de juiste invulling geven. Eigenaren moeten worden aangewezen voor/aangesproken en gecontroleerd op:
rollen;
autorisatiebeheerprocessen (in-, door- en uitstroom, rolmutatie en audit);
systemen;
data (autorisaties).</td></tr>
<tr><td>AB2</td><td>In het beleid moet zijn opgenomen op welke autorisatieclassificaties zijn onderkend. In een verdere uitwerking wordt beschreven hoe deze moet worden toegepast en wie verantwoordelijk is en welke mate van toezicht wordt vereist. Bijvoorbeeld:
<table>
<tr><td>Classificatie</td><td>Verstrekkingsbeleid</td><td>Verantwoordelijke</td><td>Mate van toezicht</td></tr>
<tr><td>“gevoelig”</td><td>least privelige met goedkeuring eigenaar per aanvraag</td><td>Autorisatie-eigenaar</td><td>Maandelijkse controle/audit</td></tr>
<tr><td>“Normaal”</td><td>goedkeuring eigenaar per rol medewerker in proces</td><td>Autorisatie-eigenaar</td><td>Reguliere controle</td></tr>
<tr><td>“Risicoloos”</td><td>Broadempowerment</td><td>Aanvrager</td><td>Geen controles noodzakelijk</td></tr>
</table></td></tr>
<tr><td>AB3</td><td>Het verdient de aanbeveling beleid op te delen in meerdere aandachtsgebieden als ‘algemeen security beleid’ en ‘autorisatiebeleid’. Het onderdeel autorisatiebeleid geeft dan concreet aan hoe met bepaalde autorisatiesituaties moet worden omgegaan.</td></tr>
<tr><td>AB4</td><td>Procuratieregels (bijvoorbeeld wie tot welk bedrag mag fiatteren) moeten helder zijn beschreven en gespecificeerd. In het autorisatietoekenningsproces moet zijn vastgelegd hoe de betreffende autorisaties in de administratie herkenbaar zijn en moet worden verwezen naar deze regels.</td></tr>
<tr><td>AB5</td><td>Het beleid moet aangeven hoe om te gaan met broad-empowerment versus least privilege (‘need to have’). Bij Broad-empowerment krijgen de (digitale) identiteiten het maximale aantal autorisaties binnen een vastgesteld risicoplafond. Bij least privilege krijgen (digitale) identiteiten alleen de strikt noodzakelijke autorisaties. Tussen deze twee uitersten zijn tussenvormen denkbaar, bijvoorbeeld:
Standaard applicatie => mag iedereen krijgen, geen goedkeuring nodig;
Autorisatie met licentieconsequenties => alleen die personen/functies autoriseren waarvoor dat echt nodig is (bijvoorbeeld per functie of per medewerker). Verstrekking geschiedt na aankoop van de licentie;
Gevoelige autorisaties => alleen die personen/functies autoriseren waarvoor dat echt nodig is (bijvoorbeeld per functie);
Beheerders autorisaties. Zijn meestal gevoelige autorisaties, zoniet dan mag hiervoor alleen broad-empowerment worden toegepast binnen de beheerdersorganisatie.
Voor het toepassen van broad-empowerment moet onderscheid worden gemaakt in autorisaties die men verkrijgt door een extra autorisatie in een autorisatie-administratie van een doelsysteem (AD, RACF, etc.) en autorisaties die leiden tot het aanmaken van nieuwe user-id’s. Het is niet wenselijk om user-id’s aan te maken die per definitie niet zullen worden gebruikt. Dat leidt tot onnodige</td></tr>
</table>

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

	beheerinspanning (kosten), geeft verwarring bij de medewerker en kosten onnodig tijd bij het uitvoeren audits.
AB6	Beleid moet beschrijven hoe om te gaan met '**need to share**'. Hierbij worden alle identiteiten geautoriseerd die vanuit hun functie mogelijk in de informatie zijn geïnteresseerd.
AB7	Beleid moet beschrijven hoe om te gaan met '**need to access**'. Hierbij wordt toegang verstrekt op het moment dat het nodig is.
AB8	Beleid moet aangeven hoe met autorisatieverstrekking moet worden omgegaan voor **directories en sharepoint-omgevingen**
AB9	In beleid moet zijn opgenomen welke regels gelden voor **functiescheiding** en hoe deze moeten worden toegepast. Functiescheidingsregels moeten zijn beschreven voor activiteiten in functies en rollen die medewerkers vervullen. In de autorisatieadministratie moet zijn aangeven op welke autorisaties welke functiescheidingsregels van toepassing zijn. Hiertoe kan een functiescheidingsmatrix worden aangelegd waarin staat aangegeven welke autorisaties niet tegelijk aan één medewerker mogen worden toegekend. Dit is regelgebaseerd autoriseren en kan centraal of soms in de applicatie geregeld worden.
AB10	In het beleid moet zijn opgenomen welke eisen worden gesteld aan de **controle** op de juistheid van verstrekte autorisaties (hoe vaak, welke wijze (goedkeuringsproces en monitoring van logging) en wanneer welke sancties). Ten behoeve van de wettelijke privacyregels dient de WBP in acht te worden genomen.
AB11	Beleid moet aangeven: - **Op welke wijze** men zichtbaar moet maken dat er aan wordt **voldaan**; **- hoe vaak** dat wordt **getoetst**.
AB12	Het beleid geeft de minimale norm voor de sterkte van het **authenticatie-mechanisme**, bijvoorbeeld: wanneer 2-factor authentication wordt vereist of welke complexiteit-eisen aan wachtwoorden worden gesteld (als het gebruik van hoofdletters of vreemde tekens). Alle systemen moeten hieraan voldoen, tenzij technologische beperkingen van een systeem dit niet mogelijk maken.
AB13	Beleid moet aangeven dat wordt nagestreefd dat medewerkers veilig **omgaan** met hun **login-gegevens** en wat daar dan onder wordt verstaan. Vastgesteld moet zijn hoe dit wordt gemeten en welke maatregelen zo nodig worden genomen (bijvoorbeeld het uitvoeren van **awareness-programma's**.)
AB14	Beleid is afhankelijk van de **cultuur**. Globaal kan worden gesteld dat beleid **branchegevoelig** is. De volgende indeling kan worden gemaakt: **Bank- en verzekeringswezen**: Behalve voor standaard werkplek autorisaties, is het beleid 'need to have'. De controle is groot op functiescheiding, de toekenning en het gebruik van autorisaties. De consequentie van verkeerde autorisaties is met name fraude. **Zorg**: Zeer open cultuur (de patiënt mag niet overlijden a.g.v. van het niet kunnen verkrijgen van de juiste informatie). Men wordt 'ruim' geautoriseerd, controle op het gebruik van autorisaties gebeurd achteraf. Consequenties van verkeerde autorisaties is voornamelijk uitlekken van medische patiëntgegevens. **Overheid**: Binnen het aandachtsgebied wordt men ruim geautoriseerd voor standaard applicaties, maar ook zijn er veel gevoelige autorisaties omtrent burgergegevens en overheidsplannen. Consequenties van beschikken over onjuiste autorisaties is het kunnen leggen van relaties tussen verschillende persoongegevens en uitlekken naar de pers van gevoelige informatie. Om dit te voorkomen is

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

	wetgeving opgesteld, bijvoorbeeld de zgn. 'Doelbindingsregistratie' en wetten gericht op het gebruik van het BSN. **Opleidingsinstituten**: veel gebruik van standaard autorisatiesets per leergang. Functiescheiding tussen leraar en leerling is groot. Kans op pogingen toch toegang te krijgen tot gevoelige informatie is groot. Consequenties van verkeerde autorisaties richten zich vooral op beoordelingsvoordeel behalen van de individuele student.
AB15	In het beleid moet zijn verwoord hoe met autorisaties van partners, klanten en leveranciers moet worden omgegaan. Denk daarbij ook aan het verstrekken van accounts aan derden die niet persoongebonden zijn (bijvoorbeeld bij extern beheer).
AB16	Beleid moet aangeven hoe met **niet persoongebonden accounts** dient te worden omgegaan. Dat betreft de goedkeuring op uitgifte, administratie, controle en gebruik hiervan.
AB17	Beleid moet beschrijven hoe **delegatie** kan worden toegepast. Welke taken mag een leidinggevende delegeren naar de onderliggende hiërarchisch laag (senior medewerkers), laten overnemen binnen de gelijke laag en welke moeten bij vervanging absoluut worden overgedragen aan de bovenliggende hiërarchische laag.
AB18	Beleid moet aangeven hoe **IT-strategie en Business-strategie** op elkaar aansluiten of in elkaars verlengde werken. Wanneer bepaalt de business en wanneer de IT-organisatie de oplossing voor een door IT te leveren service. Op volgende punten moet hiervoor een bedrijfsvisie worden beschreven: • organisatie-inrichting; • processen; • systemen en applicaties; • infrastructuur. Het verdient de aanbeveling de verantwoordelijkheid hiervoor te beleggen bij een centrale architectuurafdeling.
AB19	Beleid moet aangeven of moet worden gecontroleerd op **afwijkend inloggedrag**.
AB20	Beleid moet aangeven hoe lang **logging-gegevens**, bijvoorbeeld van inlogactiviteiten van medewerkers in doelsystemen, bewaart moeten blijven.
AB21	Beleid moet aangeven welke **flexibiliteiteisen (agility)** worden gesteld aan het vaststellen van de juiste autorisaties. Hoe snel moeten die kunnen worden vastgesteld en hoe snel moeten autorisaties kunnen worden aangepast aan: • organisatorische wijzigingen; • snel bijschakelen van grote groepen medewerkers; • herverdeling van werkzaamheden; • nieuwe marktomstandigheden; • de invoering van nieuwe systemen.
AB22	Beleid moet aangeven dat **één taal** moet worden gesproken en dat hiervoor centraal een glossary is aangelegd waarin staat vastgelegd wat er met bepaalde termen wordt bedoeld. In praktijk worden verschillende termen voor dezelfde uitleg gebruikt en anders om.
AB23	Beleid dient periodiek na gelopen te worden op toepasbaarheid als gevolg van vernieuwde eisen/wensen.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

10 ONDERKENDE KOSTEN EN BATEN

De belangrijkste driver om autorisatiebeheer op een transparante en uniforme manier in te richten, is meestal de ‘must’ om ‘in control’ te komen. Een tweede driver is kostenbesparing in de beheerorganisatie en als derde komen businessgerichte zaken als: het eenvoudiger kunnen aanvragen en het sneller verkrijgen van autorisaties. De realisatie van deze baten vindt plaats door eerst te investeren in een acces managementproject. Om te bezien of de baten groter zijn dan de kosten wordt een businesscase opgesteld.

Het soms lastig baten te kwantificeren en uit te drukken in ‘financiële opbrengsten’. Veel baten zijn indirect. Hoe wordt de snelheidswinst in het verkrijgen van autorisaties vertaald naar baten? Dit kan alleen op basis van schattingen of metingen. In nauwe samenwerking met de business en compliance officers moeten deze worden vastgesteld. Ook zijn de projectkosten lastig in te schatten. Hoeveel inspanning gaat het opstellen en invullen van een autorisatiemodel kosten?

Voor het verkrijgen van reële kengetallen is voor de start van een project een gedegen vooronderzoek nodig. Onderstaande tabellen geven kengetallen en mogelijke kosten en baten aan. De kengetallen zijn zo concreet mogelijk uitgewerkt, maar de uitwerking verschilt per bedrijfssituatie.

Kengetallen m.b.t. de huidige autorisatiebeheerorganisatie:

Nr	Omschrijving
K1	Hoeveel autorisatieaanvragen vinden er nu plaats en hoeveel tijd wordt aan de verwerking hiervan besteed (aanvragen, goed-/afkeuren en fysiek aanbrengen)
K2	Hoeveel autorisatieaanvragen zijn zoek geraakt en hoeveel tijd koste het om de aanvraag alsnog geregeld te krijgen
K3	Hoeveel wachtwoord-resets vinden er nu plaats en hoeveel tijd wordt aan de verwerking hiervan besteed
K4	Hoeveel verschillende user-id’s en wachtwoorden heeft de gemiddelde medewerker
K5	Hoeveel foutieve toekenningen vinden en er plaats en hoeveel tijd kost dit om dit te detecteren en te verhelpen (door verkeerd geformuleerde aanvraag en door foutieve handeling als verkeerde medewerker, verkeerd gebruikers-ID, etc)
K6	Hoeveel problemen doen zich voor bij het uitgeven van autorisaties die een onderlinge volgordelijke afhankelijkheid hebben

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

Algemene baten:

Nr	Omschrijving
BA1	Beter IT portfoliomanagement (inzicht in gebruikte systemen en applicaties)
BA2	Er is concreet en snel inzicht in benodigd aantal licenties
BA3	Kostendoorbelasting kan eenvoudig plaats vinden en concreet worden gemaakt
BA4	Doordat autorisaties meer consistent zijn zal het aanvraagpatroon stabieler zijn
BA5	Het aanvragen kost de business en de beheerorganisatie minder (doorloop)tijd
BA6	Auditprocessen nemen minder tijd in beslag door betere rapportages
BA7	KPI-doelstellingen kunnen eenvoudiger worden gedefinieerd en geverifieerd
BA8	Het is goed voor het bedrijfsimago als gecommuniceerd kan worden dat de goed ingerichte autorisatiebeheerorganisatie invulling geeft aan van toepassing zijnde wet- & regelgeving. Omgekeerd heeft een schandaal een zeer nadelige invloed op het bedrijfsimago en de commerciële activiteiten. De kans dat dit gebeurd wordt beperkt met goed ingericht autorisatiebeheer
BA9	Gestructureerde en/of vereenvoudigde autorisatie activiteiten kunnen in aanmerking komen voor outsourcing wat kostenbesparing kan opleveren
BA10	Doordat alle verschillende aanvraagprocessen en ondersteunende middelen (tooling) worden gecentraliseerd en centraal gefaciliteerd (één tool), worden de beheerkosten lager: • door minder mensen kan hetzelfde werk worden gedaan; • processen kunnen deels worden geautomatiseerd; • maar één tool i.p.v. meerdere (minder beheer); • één uniforme werkwijze voor de gehele organisatie (efficiënte communicatie en minder servicedesk ondersteuning); • minder handmatige handelingen (doorzetten van aanvragen, het aanbrengen van autorisaties de terugkoppeling communiceren naar de aanvrager).
BA11	De business kan sneller de juiste autorisaties aan een medewerkers toe laten kennen. Daardoor kan een nieuwe medewerker sneller met al zijn autorisaties aan de slag en kunnen wijzigingen in autorisaties sneller worden doorgevoerd, zonder teniet te doen aan juiste administraties en goedkeuringen. De agility (flexibiliteit) is hoog.
BA12	Bij goed ingericht access management is het aanbrengen van SSO eenvoudig, waardoor de gebruikers minder vaak hoeven aan te loggen
BA13	Doordat het autorisatiemanagement uniform en eventueel centraal geregeld is, is het eenvoudiger om doelgericht of gefaseerd nieuwe applicaties of systemen uit te rollen in de business.
BA14	Een access management implementatie zal het centraliseren en uniformeren van autoratieve bronnen (als personeels-, doelsysteem-, applicatie- project-, of proces-administraties) stimuleren
BA15	Vaak zijn de autorisatiemodellen op doelsystemen zeer verschillend of ongedefinieerd (langzaam ontstaan). Een access management project zal stimuleren eenzelfde autorisatiemodel na te streven op alle doelsystemen
BA16	Goed ingericht autorisatiemanagement draagt bij aan continuïteitsvraagstukken, bijvoorbeeld doordat bij een uitwijksituatie gebruik kan worden gemaakt van de centrale autorisatieadministratie i.p.v. alle lokale doelsysteemadministraties

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

Baten m.b.t. compliance

Nr	Omschrijving
BC1	Inzicht in autorisatieafkeuringen
BC2	Minder foutieve autorisatietoekenningen
BC3	Men snapt beter welke autorisaties men aanvraagt en waarom
BC4	Auditprocessen kunnen direct worden gericht op gevoelige autorisaties
BC5	Controle op fraude wordt makkelijker
BC6	Door geautomatiseerde controles (bijv. Ist-Soll vergelijking) worden ‘achterdeur’-processen in kiem gesmoord
BC7	Niet alleen de kans op fraude wordt verkleind, ook de controle op intellectuele eigendommen wordt beter en effectiever gecontroleerd. Hierdoor is de kans kleiner dat informatie bij de concurrent of in de media terecht komt
BC8	Omdat beter (continue) inzicht is in de juistheid van de verstrekte autorisaties, is de verleiding kleiner om bewust foutieve autorisaties aan te vragen
BC9	Functiescheidingsregels kunnen direct bij de start van het aanvraagproces worden gemanaged (bijvoorbeeld door functiescheidingsregels op te nemen in het autorisatiemodel). In een applicatie zelf gebeurt dit pas op het moment dat een identiteit wordt geautoriseerd, of het gebeurt achteraf bij audits (bijvoorbeeld met behulp van businessrules-tools).
BC10	Vaak worden door de implementatie van access management meerdere organisatorische vraagstukken concreet. Een veel voorkomend voorbeeld daarvan is het belegd zijn van het ‘eigenaarschap’. Voor systemen en rollen moeten eigenaren worden benoemd. Bij een bedrijfsproces-gerichte aanpak moeten proceseigenaren worden aangewezen. Zo worden verantwoordelijken expliciet en inzichtelijk.
BC11	Door het snel verstrekken van autorisaties neemt de behoefte aan non personal accounts af

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

CONCLUSIES EN VERVOLG

De leden van deze expertgroep, zie bijlage 2, hebben antwoorden geformuleerd op de gestelde vragen. Het beoogde resultaat is daarmee gehaald. De ontwikkelingen op dit vakgebied staan echter niet stil, zowel technologisch als qua visie. Deze expertbrief zal derhalve onderhavig zijn aan voortschrijdend inzicht.

De leden van de expertgroep zijn daarom altijd geïnteresseerd in opmerkingen of nieuwe inzichten nodigt u van harte uit om deze kenbaar te maken. U kunt uw reacties sturen naar expertbrief@pvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

Hoe verder?
Zoals eerder aangegeven is het onderwerp access management opgesplitst in 4 sessies met ieder een eigen set aan onderwerpen, zie bijlage 1. Ook de resultaten hiervan worden expertbrieven verwoord en via de site van het PvIB beschikbaar gesteld.

Ook via de site http://www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over access management en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

14 LITERATUURLIJST

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

Main bodies:

- Code voor Informatiebeveiliging: ISO 27001
- PI-RBAC_v_1_0a[1].pdf http://www.pvib.nl
- NIST reeks http://csrc.nist.gov/

Artikelen:

- http://www.ibpedia.nl/index.php?title=Probleemstellingen_voor_access_management
- http://www.ibpedia.nl/index.php?title=Introduction_to_access_control
- http://www.ibpedia.nl/index.php?title=Articles_about_access_control
- http://www.ibpedia.nl/index.php?title=Patterns_for_access_control
- http://www.ibpedia.nl/index.php?title=Boekbespreking_over_Studie_Role_Based_Access_Control
- http://www.ibpedia.nl/index.php?title=Special_about_controlled_access
- http://www.ibpedia.nl/index.php?title=Special_over_rolgebaseerd_autoriseren_onder_architectuur
- http://www.ibpedia.nl/index.php?title=Samenvatting_De_(on)beheersbaarheid_van_toegangsbeveiliging

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

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 hoofdgebieden 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.

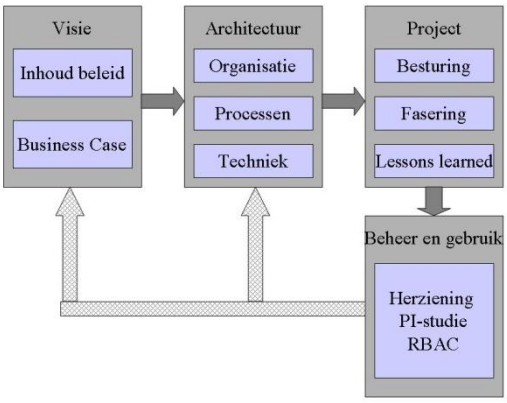


Fig. 1. Opsplitsing van onderwerp in 4 expertbrieven.

De vier hoofdgebieden behelzen het volgende:

1) Visie (deze expertbrief): 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 onderkend die het succes van een implementatieproject kunnen tegenwerken.

2) Architectuur: In het tweede onderdeel zullen architecturen worden besproken en beschreven. Dat betreft zowel de organisatie- en procesinrichting als de rolmodellering. Naast de architectuurbeschrijvingen levert de expertgroep een globale set aan functionele specificaties op voor ondersteunende middelen als tooling.

3) Project: 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 de PI-studie RBAC nader kan worden aangepast.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

BIJLAGE 2. INFORMATIE OVER DE DEELNEMERS

Jean-Pierre Vincent

Heeft als projectmanager, architect en analist sturende rollen vervult in identity & accessmanagementprogramma's. De sturing betrof zowel inhoud (oplossingen en aanpak-methoden) als projectorganisatie. De programma's werden uitgevoerd bij grote financiële instellingen met een scope van enkele tienduizenden medewerkers.

Karin van de Kerkhof

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

Tonne Mulder

Geeft leiding aan een groep medewerkers die zich bezighouden met Informatiebeveiling. Een van de aandachtsgebieden is identity & access management.

Jan-Roel Löwenthal

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.

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.

Leon Kuunders

Is als senior IAM-consultant betrokken bij de IAM-implementaties in de overheidssector. Zijn andere interesses zijn filosofie (www.despinoza.nl), corruptiebestrijding (www.transparency.nl) en openbaarheid van bestuur (www.wobverzoek.nl). Hij heeft specifieke aandacht voor het gebruiksrecht op identiteitsgegevens.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

Wiyaykumar Jharap

Is ruim 11 jaar actief in de ICT sector en heeft zich gespecialiseerd op het gebied van Security Governance, Risk & Compliance en Identity & Access Management. Voor dit laatste is hij als Senior Consultant en Projectmanager betrokken bij diverse IAM-implementaties in de industriële, energie en semi-overheidssector.

Karel van Oort

Heeft de laatste 8 jaar verschillende rollen vervuld binnen het domein van accessmanagement waaronder: autorisatiebeheerder, projectmanager, architect en adviseur. Dit bij verschillende organisaties, voornamelijk in de financiële sector.

Mike Chung

Is ruim 10 jaar werkzaam in de IT-sector en heeft verschillende functies vervuld van mainframebeheerder tot programma manager. Zijn specialismen omvatten onder meer SaaS, BPM/SOA en Open Source. Hij is een veelgevraagde spreker op congressen en seminars. In zijn vrije tijd houdt Mike zich voornamelijk bezig met ornithologie en martial arts.

Piet Kalverda

Piet Kalverda, CISSP, 23 jaar werkzaam in ICT, waarvan de afgelopen 6 jaar als Security Consultant bij een grote financiële instelling. De afgelopen 6 jaar betrokken bij ontwerp en implementatie van RBAC oplossingen als projectmanager, functioneel- en technisch specialist.

Jaap Scheepstra

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

Henk Marsman

Henk Marsman is richt hij zich in zijn werk met name op de onderwerpen van Identity & Access Management en security management. In dit werkveld adviseert hij klanten over de inzet en inrichting van identity, access en security management enerzijds en auditeert hij klanten op deze gebieden anderszijds.

Damien Meijer

Is als consultant werkzaam op het vakgebied van identity en access management.

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

18

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:

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.

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

(cc) 2009, Platform voor InformatieBeveiliging (PvIB)
This work is licensed under a Creative Commons License.