Aan: Gebruikersraad NORA

ICTU
http://www.ictu.nl

Contactpersoon
Marieke Vos

Marieke.Vos@ICTU.nl

Datum
2016-14-06

Projectnaam
NORA, katern Beveiliging

Auteur
Jaap van der Veen

memo

Wijzigingsvoorstel (RfC) NORA ten behoeve van Katern Beveiliging

Geachte leden van de Gebruikersraad,

In 2014 is het katern Beveiliging in concept opgeleverd, landelijk gereviewd en zijn de wijzigingen doorgevoerd. Wat nog rest is het actualiseren van de bestaande afgeleide principes AP 35 t/m 40, die ten behoeve van NORA-3 in 2009 afgeleid zijn van het NORA dossier Informatiebeveiliging.

Aanleiding

Actualiseren van deze afgeleide principes is nodig omdat de bestaande AP 35 t/m 40 uitsluitend het thema Informatiebeveiliging en dan ook nog slechts gedeeltelijk afdekken. Een andere reden is dat de formulering van deze principes verbetering behoeft. Tenslotte is er bij AP35 en AP 36 sprake van dubbeling.

Voorstel

Voorgesteld wordt om de huidige zes afgeleide principes met betrekking tot beveiliging (AP 35-40) te actualiseren door ze te vervangen door vijf opnieuw gedefinieerde principes: AP 35-39. Deze nieuwe principes zijn de kwaliteitskenmerken voor informatiebeveiliging, zoals die gebruikt worden in de vakliteratuur. De nieuwe principes sluiten tevens aan op de thema's Business Continuïty Management (BCM) en Privacy. Beheersmaatregelen verduidelijken de onderliggende eisen aan de organisatie-architectuur. Tevens is in deze RfC beschreven hoe IB-functies vanuit het bestaande NORA-dossier Informatiebeveiliging[1] gerelateerd zijn aan de vijf opnieuw geformuleerde afgeleide principes.

Allereerst wordt in dit document een voorstel gedaan voor uitbreiding van het kennismodel van NORA. Vervolgens wordt van elk van de vijf afgeleide principes verantwoord hoe dit wordt vervangen. De nieuwe inhoud kan gevonden worden op NORAonline.nl. De verwijzingen hiertoe staan verderop.

Verzoek

In te stemmen met dit voorstel, dan wel aan te geven met welke wijzigingen nog nodig zijn.

Met vriendelijke groet,

Jaap van der Veen
Hoofdredacteur NORA katern Beveiliging

[1] http://noraonline.nl/wiki/Bestand:NORA-dossier_IB_2010.pdf

Uitbreiding van het kennismodel NORA

Rekening houdend met de beschrijvingsmethodiek van ArchiMate, is het kennismodel van NORA uitgebreid.

Afgeleide Principes krijgen een implicatie volgens een vaste formulering om de controleerbaarheid te verhogen:
"<AP> wordt <gegarandeerd *of* gerealiseerd> door <beheersmaatregelen>".
Specifieke uitwerkingen worden gegeven in onderliggende elementen.
(ArchiMate: *Principle; a normative property of all systems in a given context, or the way in which they are realized*).

Beheersmaatregelen (ISO-2700x-term) moeten worden gehanteerd als *eisen*.
In ArchiMate termen zijn dat z.g. *Requirements*. Zij hebben als beschrijving een korte stelling.
Definitie: "Een beheersmaatregel is een verbijzondering van een (ArchiMate) requirement. Beheersmaatregelen realiseren afgeleide principes."
(ArchiMate: *Requirement; a statement of need that must be realized by a system).*
Beheersmaatregelen hebben als stelling een beschrijving van een eis waaraan voldaan moet worden om het bovenliggende principe te realiseren.
Eigenschappen van beheersmaatregelen zijn:

- Stelling
- Toelichting
- Implicaties

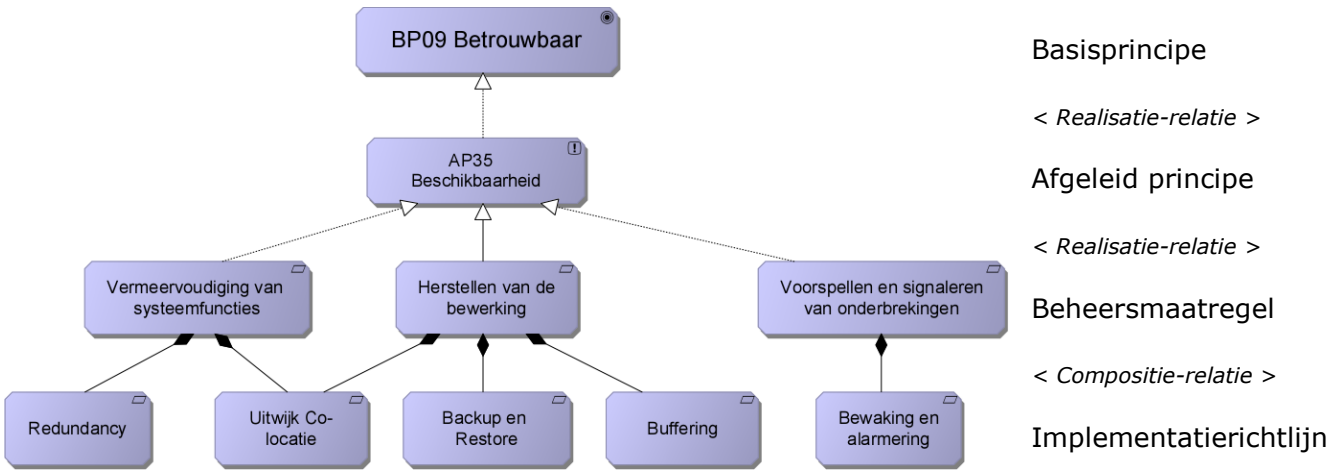
Implementatierichtlijnen worden toegevoegd als *eisen*.
In een *compositierelatie* realiseren implementatierichtlijnen de beheersmaatregel.
Definitie: "Een implementatierichtlijn is een verbijzondering van een (ArchiMate) requirement. Implementatierichtlijnen expliciteren beheersmaatregelen. Zij fungeren als ontwerp- en toetsingsnorm en zijn het meest concrete abstractieniveau in het katern Beveiliging, op het grensvlak van 'WAT' en 'HOE' van normenkaders."
Eigenschappen van implementatierichtlijnen zijn:

- Stelling

Mogelijke relaties

- Beheersmaatregel realiseert Afgeleide Principes
- Beheersmaatregelen zijn gegroepeerd door Beheersmaatregelen (compositie)
- Implementatierichtlijnen zijn gegroepeerd door Beheersmaatregel (compositie)

Nota bene:
De huidige Basisprincipes zijn vergelijkbaar met ArchiMate 'doelen' (ArchiMate: *Goal; an end state that a stakeholder intends to achieve*). Voorstel is om, in afstemming met Katern Verbinden de Basisprincipes in het kennismodel te noemen als doelen, terwijl ze de naam 'basisprincipe' behouden. Op die manier volgt het kennismodel ArchiMate, zonder dat de bekende term vervalt.



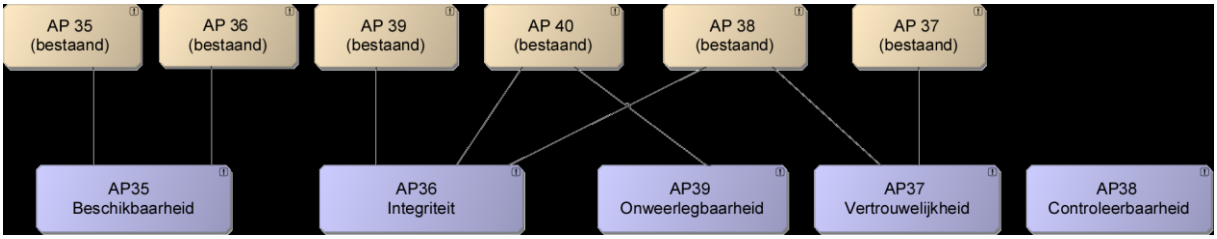
Figuur 1 Voorbeeld principes en relaties in het katern Beveiliging

Figuur 1 geeft een voorbeeld-uitwerking van een deel van het katern. Bovenaan staat het bestaande basisprincipe BP09: Betrouwbaarheid. De inhoud van dat basisprincipe komt overeen met die van een ArchiMate-doel, maar we gebruiken in het katern het NORA-begrip "Principe". Betrouwbaarheid wordt onder andere gerealiseerd door het (afgeleide) principe Beschikbaarheid. Beschikbaarheid wordt beschreven door de stelling: '*De beschikbaarheid van de dienst voldoet aan de met de afnemer gemaakte continuïteitsafspraken*'. Het principe Beschikbaarheid wordt gerealiseerd door een aantal beveiligingseisen (beheersmaatregelen), waaronder de eis 'bewerkingen zijn herstelbaar'. Deze beveiligingseis wordt gerealiseerd door een set van eisen (implementatierichtlijnen), zoals 'berichten worden gebufferd'.

Vervanging van de bestaande Afgeleide Principes

De bestaande AP's 35 t/m 40 worden vervangen door nieuwe afgeleide normatieve principes. Deze nieuwe principes dekken het aandachtsgebied informatiebeveiliging in z'n geheel af en zijn generiek vertaalbaar naar alle onderliggende beveiligingsfuncties. Ze kunnen daarom in een organisatie gelden voor alle systemen, bedrijfsprocessen, gegevens en het gebruik daarvan door klanten en medewerkers. Het zijn tevens geaccepteerde begrippen in het vakgebied Beveiliging.

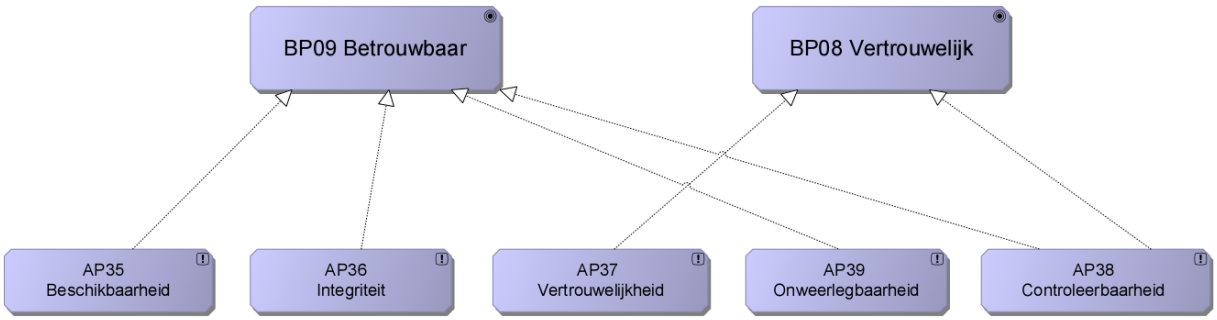
Aan de nieuwe principes zijn de bestaande nummers toegekend. Figuur 2 geeft aan welk bestaand principe wordt vervangen door welk nieuw afgeleid principe. Een cross-reference lijst geeft aan waar de verschillende stellingen, rationale en implicaties van de bestaande principes terug komen in de nieuwe opzet.



Figuur 2 Vervanging van afgeleide principes AP 35 t/m AP 40

Relatie basisprincipes en nieuwe Afgeleide Principes

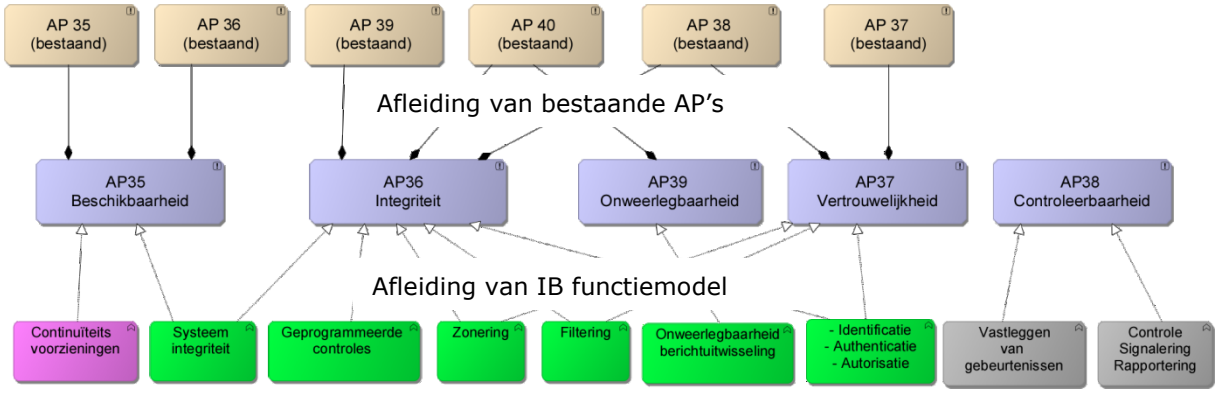
Figuur 3 schetst de relatie tussen de basisprincipes BP08, BP09 en de nieuwe afgeleide principes. Wat opvalt is dat er verschillende kruisverbanden bestaan tussen de principes. Ook hier is voor basisprincipes het ArchiMate symbool van 'Doel' aangehouden, omdat in de ArchiMate-taal een 'onderliggend' principe niet een ander of 'bovenliggend' principe kan realiseren.



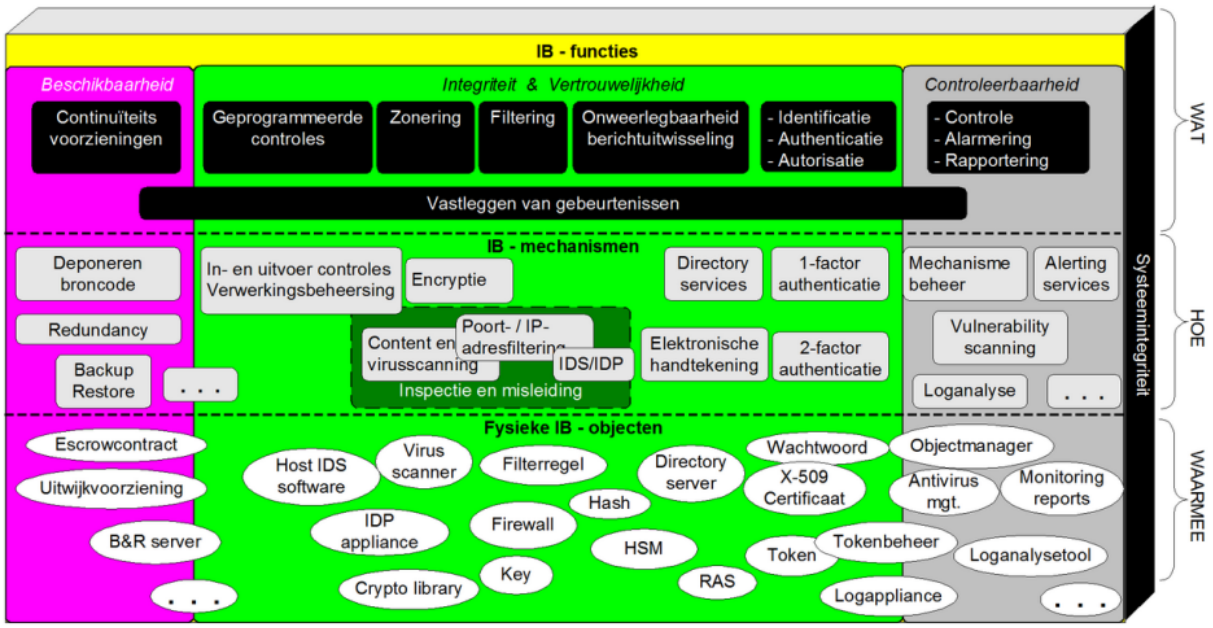
Figuur 3 Relatie van basisprincipes en nieuwe afgeleide principes

Afleiding van bestaande AP's en IB-functies

De bestaande AP's 35 t/m 40 zijn in 2009 afgeleid van het NORA dossier Informatiebeveiliging, waarbij het IB-functiemodel van Figuur 5 centraal stond. Het nieuwe katern Beveiliging is een doorontwikkeling van het dossier Informatiebeveiliging. Figuur 4 schetst hoe de oorspronkelijke beveiligingsfuncties uit het dossier de nieuwe afgeleide principes realiseren.



Figuur 4 Afleiding van bestaande AP's en beveiligingsfuncties naar nieuwe AP's



Figuur 5 IB-Functiemodel van het NORA-3 dossier Informatiebeveiliging

In het nieuwe katern komen de "WAT – HOE – WAARMEE" voorbeelden terug in de architectuurviews (in ArchiMate symbolen) die nog worden toegevoegd aan de huidige content van de Wiki. (zie punt 3 van nog uit te werken onderdelen).

Op termijn nog uit te werken onderdelen

Geen onderdeel van het huidige wijzigingsverzoek zijn de volgende niet-normatieve onderdelen:

1. “Views”, thema-pagina’s om een ingang te bieden tot de content. Dit kan langs beveiligingsfuncties zoals Scheiding, Systeemintegriteit, Applicatieve Controle, Continuïteit, Filterfuncties en Toegangsfuncties. De intentie is om deze in het volgend stadium op te nemen. Daarbij zullen ArchiMate-platen worden getoond met een set van beheersmaatregelen, implementatierichtlijnen en hun bovenliggende principes, alsook een verwijzing naar mogelijke applicaties en services die gerelateerd zijn.
2. Voorbeelden. Gebruikers worden uitgenodigd om hun eigen voorbeeldverhalen aan te dragen die gekoppeld kunnen worden aan principes, beheersmaatregelen of implementatierichtlijnen. Deze zullen als kleinere wijzigingen door NORA Beheer worden toegevoegd als aparte pagina’s.
3. Archimate symbolen moeten worden toegevoegd aan de huidige content van de Wiki; de voorbeeldoplossingen.

BIJLAGE – Reviewprocedure

Ter herinnering: aansluitend bij het reviewproces van NORA (http://noraonline.nl/wiki/Reviewproces), zal het richtinggevende deel van het katern de komende maanden in review worden gegeven.

Zoals in de bijeenkomst van de Gebruikersraad NORA van 12 februari 2014 is aangekondigd, wordt het volgende reviewproces doorlopen:

- Gebruikersraad NORA geeft akkoord voor review, eventueel met opmerkingen op hoofdlijnen (twee weken).
- De conceptversie wordt formeel gepubliceerd op NORA online ter review (begin maart).
- In publieke review (maart-april) krijgen geïnteresseerden de kans om opmerkingen in te sturen. De Gebruikersraad, samen met NORA beheer en de expertgroep, gebruikt haar netwerk om betrokkenen op te roepen te reageren.
- NORA beheer verzamelt de feedback voor de expertgroep beveiliging.
- Begin april worden de eerste, mineure opmerkingen alvast verwerkt in de wiki. De doelgroep wordt opnieuw op de hoogte gesteld, waarbij de motivatie voor de mineure opmerkingen wordt meegegeven. Dit beperkt dubbeling in opmerkingen, versnelt de review en brengt het katern extra onder de aandacht.
- Medio april wordt review gesloten. De expertgroep beoordeelt de commentaren gezamenlijk. Commentaren van vertegenwoordigers uit de Gebruikersraad wegen hierbij zwaar.
- De expertgroep verwerkt de commentaren plus beoordeling in een nieuwe versie van het katern.
- De uiteindelijke versie wordt ter instemming voorgelegd aan de Gebruikersraad op 14 mei 2014.