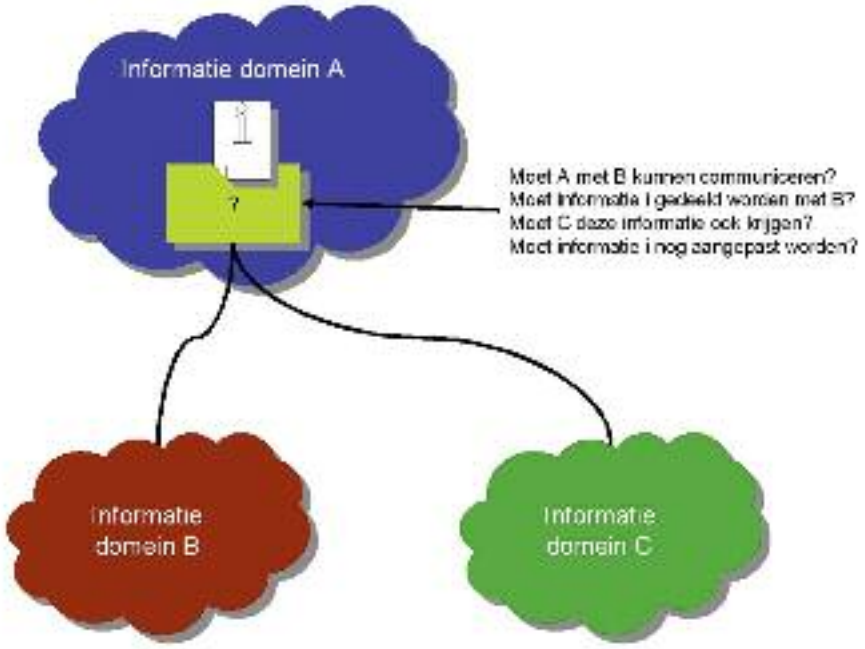
RUBRICEREN BOTTLENECK VOOR INFORMATIEDELING

Ir. A.C.M. Smulders, TNO-ICT

Ir. A.C.M. (Andre) Smulders is sinds 1996 werkzaam in diverse rollen binnen het ICT-vakgebied en sinds 2000 op het gebied van informatiebeveiliging. Hij is momenteel werkzaam als *Senior Consultant Security* binnen de afdeling *security* van TNO-ICT. Hij is programmaleider van het onderzoeksprogramma informatiebeveiliging voor Defensie en trekker van het onderwerp *cyber security* binnen TNO. De auteur werkt aan diverse *security*- en informatiebeveiligingsprojecten voor zowel Defensie als voor andere markten. Het op een andere wijze omgaan met rubricering is een essentiële voorwaarde om dynamisch risicomanagement op informatie toe te kunnen passen om de stap te kunnen maken naar *duty to share*.

Binnen de IV verkenningen 2020 wordt aangegeven met welke concrete vragen Defensie wordt geconfronteerd. Een kernvraag daarin is hoe Defensie ervoor zorgt dat met dezelfde middelen informatie kan worden uitgewisseld met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en met coalitiepartners in een uitzendgebied. Daarbij komt dat in de uitvoering van haar taken, de samenwerking op een steeds lager niveau in de organisatie plaatsvindt. Er zijn diverse ketens waarbinnen Defensie een belangrijke rol heeft. Daarmee wordt ook informatieuitwisseling tussen onderdelen van die ketens steeds belangrijker. Waar voorheen informatie 'aan de borst' werd gehouden, neemt de noodzaak tot het delen van informatie toe.

Deze nieuwe kijk op informatiedeling vraagt om nieuwe manieren waarop informatie beveiligd wordt. De traditionele benadering hierin is het beoordelen van informatie gericht op het afschermen van de buitenwereld. Binnen het nieuwe paradigma zal de focus daarentegen moeten liggen op het beoordelen van informatie gericht op het delen en beschikbaar stellen.
Het bij het nieuwe paradigma behorende beleid richt zich op zaken als *'duty to share'* en 'open tenzij'. Om succesvol te zijn, zullen deze beleidsuitspraken geïmplementeerd moeten worden. Een randvoorwaarde voor een succesvolle implementatie van deze beleidsuitspraken is het kunnen definiëren van criteria die aangeven of het beleid succesvol behaald wordt. Overigens zal ook binnen deze benadering nog steeds niet alle informatie open zijn voor iedereen. Dit betekent voor de beleidsimplementatie dat in het kader van 'open tenzij', als eerste stap criteria opgesteld moeten worden die aangeven wat 'tenzij' inhoudt en onder welke voorwaarden hieraan voldaan wordt.
Het beleggen (of implementeren) van deze criteria en randvoorwaarden kan vervolgens verschillende vormen aannemen zoals bijvoorbeeld organisatorisch of technisch. Een voor de hand liggende volgende stap is dan ook het bepalen waar deze implementatie het meest effectief en efficiënt uitgevoerd kan worden. Te verwachten is dat dit een *'multilevel'* aanpak zal worden waarbij er een balans gezocht zal worden tussen verschillende vormen van implementatie. Essentieel bij de keuze om de criteria en randvoorwaarden technisch te implementeren, is dat deze vast te leggen zijn in een *policy*. Technische oplossingen moeten vervolgens op basis van zo'n *policy* in staat zijn de juiste beleidskeuzes te faciliteren.
(Technische) beveiligingsmechanismen moeten in staat zijn een beleidsuitspraak af te kunnen dwingen ook als die beleidsuitspraak bijvoorbeeld inhoudt dat alles gedeeld moet worden. De ontwikkeling van beleid loopt daarbij niet synchroon met de ontwikkeling van de techniek. Daarom zullen beveiligingsmechanismen zodanig ontwikkeld moeten worden dat deze in staat zijn om de gewenste *policy* te ondersteunen. Om dit mogelijk te maken zullen deze technische componenten in staat moeten zijn om informatie inhoudelijk te beoordelen dan wel op basis van meta-informatie beslissingen kunnen nemen in lijn met een vanuit de beleidslijn opgelegde *policy*.
De plaats waarop beleidsafspraken geïmplementeerd zullen worden is op de grens tussen informatiedomeinen. Hierbij dient opgemerkt te worden dat er nog geen sluitende definitie van informatiedomeinen is die hier als basis kan dienen. De facto ligt de grens van een informatiedomein nu in veel gevallen nog bij de technische netwerkgrens. De rol van de mechanismen op dit grensvlak is het implementeren van het beleid. Bijvoorbeeld er voor zorgen dat informatie overgedragen wordt naar de partijen die dit conform afspraak moeten ontvangen, zoals is weergegeven in figuur 1.



Figuur 1. Beleidsuitspraken in relatie tot beveiligingsmechanismen

De huidige vorm van rubriceren is gericht op het aan informatie koppelen van een label (zoals NATO SECRET, Departementaal Vertrouwelijk). Het beleid schrijft vervolgens voor hoe die informatie behandeld dient te worden. De rubricering wordt bepaald door de steller of de bron van de informatie. Het beoordelen van deze rubricering kan in de huidige situatie alleen door de bron plaatsvinden. Dit is logisch want anders zou een bron de informatie nooit kunnen delen met een andere partij. Een bron deelt informatie immers alleen als deze er vertrouwen in heeft dat zijn informatie in dezelfde mate beschermd wordt als hij zelf zou doen. Een consequentie hiervan is dat een andere bewerker op basis van de rubricering en de inhoud niet kan bepalen of er in de toekomst met de inhoud of rubricering van het document anders kan worden omgesprongen.

De reden voor deze beperking zit in het de doelstelling waarmee de rubricering is toegekend. Hierin zijn grofweg verschillende onderverdelingen te maken waarvan hieronder twee voorbeelden gegeven worden:

- de rubricering is gerelateerd aan de inhoud van de informatie;
- de rubricering is niet zozeer gerelateerd aan de feitelijke inhoud van de informatie, maar zegt iets over de *capabilities* of bronnen van degene die het document opstelde.

Het eerste principe is in de nieuwe situatie nog steeds toepasbaar het tweede niet. Om dit verschil inzichtelijker te maken het volgende voorbeeld weergegeven in figuur 2.

Een sensor stuurt videobeelden van een lege woestijn naar een basisstation. De ontvanger zal op basis van een inhoudelijke beoordeling stellen dat er geen gevoelige informatie te herkennen is in het videobeeld en gedeeld kan worden in het partner domein. De resolutie van deze videobeelden kan echter een *capability* zijn die een belangrijk *intelligence* voordeel oplevert en dus beschermd moet worden. In de huidige situatie leidt dit tot het rubriceren van de sensor data waarmee deling beperkt wordt tot een kleine kring, namelijk het verwerkingsdomein.

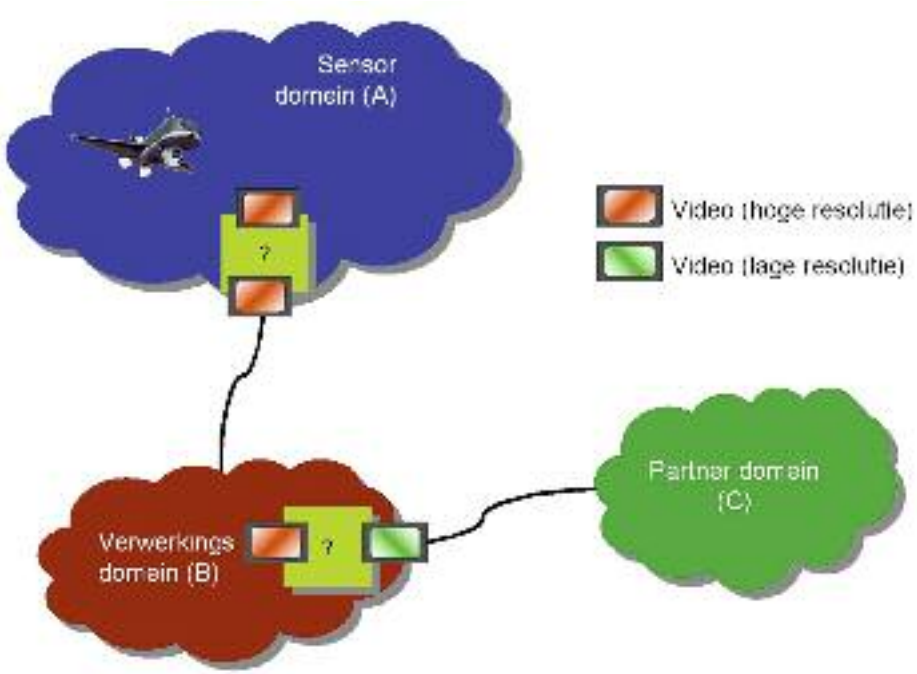
In het nieuwe model zou een mechanisme ingezet kunnen worden dat automatisch deze *capabilities* aanpast (bijvoorbeeld door de beelden te *resampelen* naar een lagere resolutie) waardoor de informatie wél gedeeld kan worden.

Overigens zou vandaag de dag met dit voorbeeld waarschijnlijk in de praktijk hetzelfde gebeuren: na overleg met de bron zou een gedeclassificeerde versie gemaakt worden op een lagere resolutie. Het punt dat we hier proberen te maken, is dat door toenemende eisen aan snelheid van communiceren, ruggespraak in de hierboven geschetste nieuwe manier van opereren, niet meer houdbaar is. Om dit mogelijk te maken moet het informatiemanagement systeem beschikken over de achterliggende reden van de classificering. Bij transport naar een ander geclassificeerd of ongerubriceerd domein kan dan de juiste toets aan het beleid gemaakt worden en voorafgaand aan de overdracht toegepast worden.

Merk hierbij op dat *capabilities* een zeer breed begrip is en zeker niet eenvoudig te duiden. Het is echter wel noodzakelijk om hier grip op te krijgen zeker als de rol van informatie eigenaar als gevolg van het nieuwe paradigma verandert of in een aantal gevallen misschien niet meer vast te stellen is. Het is dan ook van belang om bij de bron van de informatie aan te kunnen geven welke *capabilities* beschermd moeten worden en dit mee te geven aan de verwerker van de informatie. Vervolgens kan op basis hiervan in combinatie met een inhoudelijke beoordeling de juiste risico afweging gemaakt worden, die vervolgens ook nog getoetst kan worden aan een *policy* voor informatiedeling.

De conclusie is dat, wanneer de focus verschuift van het *beschermen* van informatie naar het delen van informatie, een nieuwe visie noodzakelijk is op informatiebeveiliging. Kernbegrippen daarin zullen moeten zijn: de functie van rubricering c.q. labelen, de inhoud en vastlegging van het begrip *'capability'* en de invulling van het begrip informatie-eigenaarschap. Vervolgens zullen er nieuwe methodieken en technische middelen moeten worden gezocht die in staat zijn om beleidslijnen te implementeren en daarmee de invulling van het beleid handen en voeten te geven.

Het op een andere wijze omgaan met rubricering is een essentiële voorwaarde om dynamisch risicomanagement op informatie toe te kunnen passen. De huidige vorm van rubriceren geeft zoals hierboven geschetst te weinig handvatten om los van de bron de juiste belangen af te kunnen wegen die bij een dynamische risico afweging noodzakelijk is.



Figuur 2. Informatiedomeinen en beveiligingsmechanismen

BRONNEN:

- Informatievoorziening bij Defensie. Een doorkijk naar 2020. Rapport in het kader van de Verkenningen, 3 februari 2009