SILVER BULLET FOR INFORMATION SHARING

Arnold Colijn, Sr Projectmanager Innovatie DMO/JIVC/KIXS[1]

Informatie is het nieuwe wapen! Een wapen dat de mentale component kan beïnvloeden, maar dat ook essentieel is voor besluitvorming en een tijdige fysieke impact. De vraag wie wanneer toegang moet hebben tot welke informatie houdt ons al tijden bezig. *The need to share balanced by the need to know*. Hoe kun je die balans vinden en wat is er nodig? In dit artikel beschrijven we de zoektocht naar een *Silver Bullet,* waarmee we technisch gezien in staat zijn om bidirectioneel informatie uit te kunnen wisselen tussen netwerken met een verschillend rubriceringsniveau of met een andere eigenaar. We zijn heel ver en tegelijkertijd staan we aan het begin. Naast de techniek is er nog een wereld te winnen. Bij het gebruik van de technische mogelijkheden zal er genoeg discussie ontstaan waar de balans moet liggen. Zoek je mee? ➔

Verschuivende balans

Kort na zijn aantreden mocht ik een presentatie geven voor onze huidige CDS over het project Generiek Koppelvlak voor hoog gerubriceerde informatie-uitwisseling (HGI). Na een vlammend betoog was de nuchtere reactie: "*Jij gaat dus op zoek naar de Silver Bullet, dat willen we al jaren, veel succes ermee*"! Nu kun je hier onzeker van worden, maar in deze wereld moeten we juist met onzekerheid om leren gaan. Informatiegestuurd optreden op basis van een gezaghebbende informatiepositie, multidomein en geïntegreerd is een hele mond vol. Daar kom je niet zonder pionieren. De '*need to share*' neemt enorm toe, terwijl de behoefte blijft bestaan om de integriteit en exclusiviteit van de informatie te verzekeren.

De balans tussen delen en beschermen van informatie komt ook naar voren in de probleemanalyse van de Defensievisie 2035: '*We lopen het risico te verdrinken in de zeeën van informatie.*' en '*Onze digitale en fysieke infrastructuur is niet goed beschermd tegen (toekomstige) dreigingen.*' De grote hoeveelheid beschikbare data overweldigt ons en we zijn bang dat we de boot missen en een inferieure informatiepositie krijgen. Er gaat veel aandacht uit naar het verzamelen, opslaan, verrijken en analyseren van de grote hoeveelheden data. De kans op serendipiteit[2] is gigantisch. Tegelijkertijd stelt het ons voor een aantal vragen: hoe integer is de data die we binnenhalen en versturen; is de bron wel te vertrouwen; kunnen we informatie wel afschermen voor de tegenstander en toegankelijk maken voor onze eigen mensen?

Waarom

De vraag wie toegang moet hebben tot welke informatie doet me terugdenken aan een les tijdens de officiersopleiding. Vrij vertaald kwam het hier op neer: bij informatie-logistiek gaat het er om dat je de juiste informatie op de juiste tijd op de juiste plaats bij de juiste actor in de juiste hoeveelheid krijgt, gericht op de taak en het doel waar die actor voor is aangesteld. 'Juiste informatie' stond daarbij voor allerlei kwaliteitskenmerken zoals beschikbaarheid, integriteit, exclusiviteit, relevantie en gerichtheid. Ondanks de toenemende behoefte om informatie te delen is er ook een behoefte om bepaalde essentiële informatie af te schermen, zelfs voor bondgenoten. Het verzamelen, fuseren, analyseren en verrijken van data leidt er al snel toe dat het netwerk waarop dit gebeurt een hogere rubricering krijgt. Binnen zo'n netwerk of binnen een federatie van vertrouwde netwerken zijn verschillende maatregelen mogelijk om op een veilige manier informatie met elkaar te delen.

In veel gevallen willen we echter ook samenwerken met partners waarbij we de gebruikte netwerken niet vertrouwen. Dit kan zijn omdat het bijvoorbeeld een andere eigenaar heeft of een andere rubricering. De uitwisseling van informatie vindt dan plaats op wat we vaak aanduiden als een *Information Exchange Gateway* (IEG). In de toekomst doen we dit bijna realtime en veelal zonder menselijke tussenkomst. Hierin moeten we een grote sprong gaan maken. In het project ontwikkelen we een datafilter waarmee op basis van vooraf goedgekeurde regels bepaald kan worden of informatie wel of niet kan worden gedeeld met de ontvanger. Het datafilter is een *high assurance* onderdeel van de totale IEG. Daarmee beschermen we onze hoog gerubriceerde data en bieden we de mogelijkheid om bidirectioneel de juiste informatie met de juiste ontvanger te delen. De IEG draagt voor de *duty to share* bij aan de integriteit- en voor de *need to know* aan de exclusiviteit van de informatie.

Waar komen we vandaan

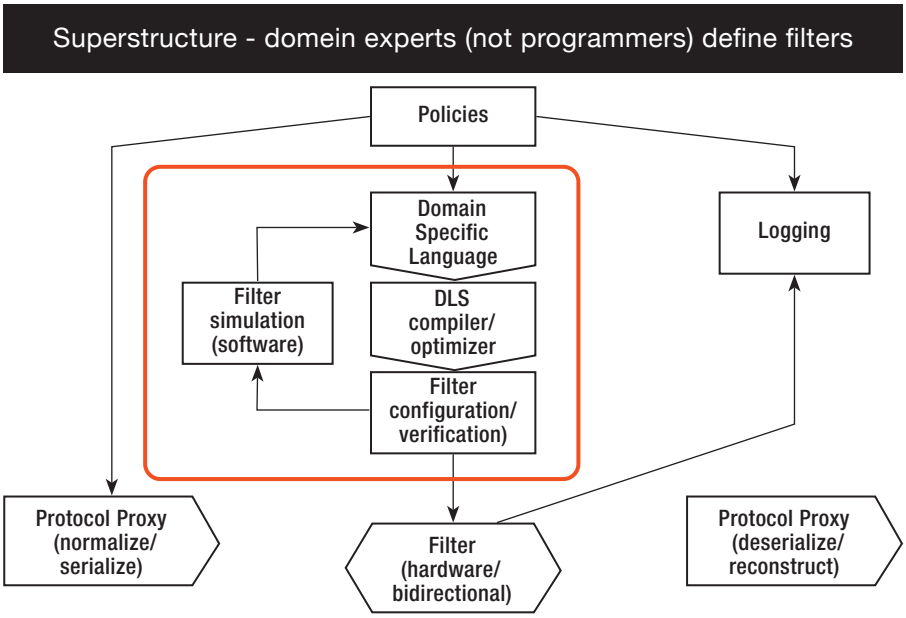
Deze uitdaging is niet nieuw. In de dossiers van opeenvolgende schatzoekers is er al een artikel van overste Bertelink uit 2012 die een beschrijving geeft van de security functionaliteiten waaruit een generiek koppelvlak kan worden opgebouwd. In de jaren daarna zijn verschillende studies, technische beproevingen en marktanalyses gedaan om een oplossing te vinden. In 2018 is er een *Proof of Concept* opgeleverd met twee marktpartijen, waarbij het eindoordeel was dat er een doorontwikkeling nodig is van één van de oplossingen. De behoeftestelling hiervoor heeft een flinke aanloop genomen. In een tijd van schaarste is het niet eenvoudig om een risicovol project 'boven de streep' te trekken. In deze fase is de gezamenlijke inspanning gestart tussen de innovatieclub KIXS en de sectie HGI. Er is in 2020 een opdracht gekomen voor het maken van een *software demonstrator* en een eerste systeemontwerp. De resultaten van dit vooronderzoek gaven voldoende vertrouwen om het jaar daarna het project CDS.IV.444 Generiek Koppelvlak HGI op te starten. Het project borduurt voort op de eerdere studies en het vooronderzoek. Het doel van het project is breed geformuleerd: Verbeteren van interoperabiliteit en bijdragen aan Informatiegestuurd optreden (IGO), door veilige uitwisseling van informatie tussen ongelijkwaardig gerubriceerde domeinen mogelijk te maken. Juist omdat het gaat om het ontwikkelen en gebruiken van nieuwe technologie is het exacte resultaat niet vooraf af te geven. Het is daarom essentieel dat de leverancier Technolution goed begrijpt wat de context en het belang is van Defensie bij het ontwikkelen van deze technologie.

Waar zijn we mee bezig

Het project realiseert een hardwarematig datafilter samen met Technolution en begeleid door een Ontwikkel- en Begeleidingsteam (OBT) van het Nationaal Bureau voor Verbindingsbeveiliging (NBV). Het gewenste projectresultaat is een certificeerbare bouwsteen voor datafiltering binnen een *Information Exchange Gateway* (IEG). Dit betreft een generiek hardwarematig

datafilter voor *high-assurance* koppelingen tussen ongelijkwaardig gerubriceerde systemen. Het datafilter is in staat om gestandaardiseerde XML-berichten te controleren op basis van een gedefinieerde policy. Het datafilter is voor alle soorten discrete bericht-data programmeerbaar. Naast het ontwikkelen van het datafilter levert het project ook een blauwdruk voor alle DOTMPLFI-aspecten. De scope van het project is beperkt. Als uiteindelijk de bouwsteen voor datafiltering gereed is moet deze nog worden ingebed in de totale keten waarmee de IEG wordt gevormd. De ondersteuning vanuit het NBV is essentieel, omdat er een grote kennis aanwezig is van potentiele dreigingen en risico's, ook op technisch niveau, die maar weinig mensen kunnen overzien. Daarnaast adviseren zij Defensie over de opzet van de processen die deel uitmaken van de evaluatie. Tijdens de ontwikkeling zijn diverse *developmentpartners*[3] betrokken om het datafilter te beproeven. De beproevingen moeten niet alleen de werking aantonen van het hardwarematig datafilter, maar ook inzicht geven in de voor- en na bereiding van de informatiestromen om een beeld te krijgen voor toekomstige usecases op de roadmap.

Om de ontwikkeling van het datafilter gelijk te laten lopen met de ontwikkeling van de omliggende keten van de IEG, ook wel proxyframework genoemd, is in het programma Grensverleggende IT (GrIT) besloten om de ontwikkeling van dat proxyframework naar voren te halen in de planning. Dit zorgt er voor dat de architectuur goed op elkaar is afgestemd. Binnen de scope van GrIT is Defensie zelf verantwoordelijk voor het leveren van het hardwarematig datafilter of datadiodes[4]. Naast het technische ontwikkeltraject wordt ook de organisatie voorbereid voor het generiek koppelvlak. In de huidige reorganisatie van het JIVC wordt een *Data Exchange Office* (DEO) vormgegeven. De eerste drie urgente functies zijn al vrijgegeven om tijdens de ontwikkeling van de techniek ook de processen uit te werken en kennis op te doen over het begeleiden van de usecases. Het *Data Exchange Office* is een nieuw team binnen DMO/JIVC/BOO IT dat zich bezighoudt met het uitwisselen van hoog beveiligde informatie tussen ongelijkwaardige netwerken. Het team is verantwoordelijk voor het ontwikkelen, testen en uitleveren van de technische implementatie van deze data-uitwisseling. Daarnaast begeleidt het DEO de informatie-eigenaren bij het accreditatieproces. Bij het ontwikkelen van de processen moet een risicoanalyse bepalen hoe de rol- en taakverdeling worden vormgegeven.



Wat maakt het koppelvlak generiek

In de toekomstige IEG is het mogelijk om het hardwarematig datafilter te programmeren, testen en configureren voor een specifieke usecase. In de figuur is dit weergegeven in het rode kader. Dit betekent dat niet meer voor iedere usecase een maatwerkoplossing hoeft te worden gemaakt en dat het mogelijk wordt om kennis van de eerder gebruikte protocollen en libraries te hergebruiken. De berichtuitwisseling tussen applicaties wordt afgepeld naar het gewenste bericht en vertaald naar een gestandaardiseerd tekstbericht (veelal XML) waar vervolgens de filters op worden toegepast. De rol voor de domeinexperts is om de behoefte aan filtering te bepalen. Dit is waarmee uiteindelijk de policies voor informatie-uitwisseling worden ingevuld. Dit proces wordt ondersteund door een policy-editor. Na deze stappen wordt de usecase door de informatie-eigenaar voorgelegd voor accreditatie. Bij akkoord kan de policy worden *gesigned* en deze wordt vervolgens ingeladen in het filter. Voor iedere usecase kan gebruik worden gemaakt van dezelfde geëvalueerde generieke hardwarecomponenten en interfaces, omdat het programmeerbare hardware betreft.[5]

Deze IEG wordt gebruikt voor informatie-uitwisseling tussen netwerken, waarbij sprake is van een verschillend rubriceringsniveau of een verschillende eigenaar. Het betreft dus nog steeds een meer generieke point to point oplossing, waarbij het vanwege de gekozen technologie wel mogelijk is om tussen de twee netwerken bidirectioneel meerdere datastromen te laten lopen. Met de oprichting van het *Data Exchange Office* is de intentie om niet alleen een generieke technische oplossing te bieden, maar ook de procesgang voor accreditatie en het beheer van de koppelvlakken te accommoderen.

Wat betekent het voor Defensie

Voor Defensie ontstaat de mogelijkheid om bidirectioneel informatie uit te wisselen, dus ook van 'hoog naar laag' en dan wel op een manier die voldoende vertrouwen geeft dat alleen die informatie wordt doorgelaten die voldoet aan de gestelde voorwaarden. Hiermee ondersteunt het de behoefte om relevante informatie te delen naar operators of effectoren. Zeker bij tijdkritische informatie kan dit van grote

waarde zijn bij het huidige en toekomstige optreden. Om dit te bereiken zijn er nog wel een paar stappen nodig. Voorafgaand aan de uitwisseling van informatie tussen twee partijen zal hier altijd eerst overeenstemming over moeten zijn. Dit wordt vaak vastgelegd in een *Memorandum of Understanding*. Dit vormt de basis om specifiek te kijken welke informatiestromen uitgewisseld kunnen worden en onder welke voorwaarden berichten al dan niet gedeeld mogen worden. Dit vergt kennis van de operationele context gecombineerd met kennis van de opbouw van protocollen en berichten. De domeinexpert definieert het filter en de programmeur helpt de domeinexpert met behulp van de policy-editor om de opbouw van de berichten te overzien. Deze stappen zijn vooral van belang wanneer we informatie van een hogere rubricering naar een lagere willen sturen, of wanneer we het netwerk van een partner niet vertrouwen.

Naast de inhoudelijke analyse van de structuur van de berichten is het ook nodig om protocollen geschikt te maken voor transport naar het filter. Vanuit het proxy framework wordt hier een *Software Development Kit* (SDK) aangeleverd en door het DEO wordt gezorgd voor zoveel mogelijk hergebruik van het werk dat hierin is gedaan. De processen voor aanschaf, configuratie, opleiding, gebruik, beheer en afstoting worden nog verder ontwikkeld in samenwerking tussen het project, GrIT en het DEO. Het project Generiek Koppelvlak HGI heeft de scope om het datafilter te ontwikkelen, zodat het beschikbaar komt op de markt. Voor de aanschaf en exploitatie is een ruwe kosteninschatting gemaakt, zodat toekomstige gebruikers een budget kunnen reserveren voor hun behoeftes. Het uitwerken van de usecases zal zeker in het begin de nodige inspanning vergen, waarbij de CIO-office waar nodig prioriteiten zal stellen voor de roadmap.

Waar gaan we naar toe

De primaire focus van het project is op de informatie-uitwisseling van gestructureerde berichten. Het is echter ook mogelijk om ongestructureerde berichten te releasen op basis van labels. In NATO-verband worden hiervoor STANAGs vastgesteld om de interoperabiliteit te waarborgen. Binnen GrIT worden de voorbereidingen getroffen om dit mogelijk te maken en in het project wordt met deze ontwikkeling ook rekening gehouden. Bij dit soort uitwisseling is het lastiger de exclusiviteit te waarborgen en is het vaak nodig om aanvullende maatregelen te nemen, zoals het aanstellen van een release-officer, het integraal loggen van berichten of geautomatiseerde controles op de inhoud om over de releasebeslissing te adviseren of zelfs deze beslissing door het systeem te laten nemen. Er bestaat ook een grote behoefte om over ongelijkwaardige netwerken real-time informatie uit te kunnen wisselen (video/spraak). De mogelijkheden om hier datalekken te voorkomen zijn echter beperkt, dus in de totale risico-afweging moeten hier veel meer onderwerpen worden meegenomen dan alleen de techniek. Er start binnenkort wel een *Proof of Concept* om de technische mogelijkheden te verkennen die deze behoefte kunnen ondersteunen in een nieuw innovatieproject bij DMO/JIVC/KIXS.

Hoe vinden we de balans

Op dit moment steken we veel energie in het mogelijk maken van een veilige informatie-uitwisseling. De *need to share* is enorm toegenomen, maar de technische mogelijkheden hiervoor zijn beperkt. Het is vaak de operationele commandant die op basis van de eigen risico-inschatting informatie deelt. Mijn verwachting is dat een goede analyse van de behoefte aan het delen van informatie tot een andere risicohouding kan leiden van alle betrokkenen. Veel informatie in een hoog gerubriceerd netwerk is op zichzelf niet hoog gerubriceerd en als het belang van het delen van informatie prevaleert boven het exclusief houden van informatie kan er wellicht worden gekeken naar harmonisering van het rubriceringsniveau. Het kan dus ook zo zijn dat er vanwege het belang van het delen van informatie wordt gekozen om een netwerk een hogere rubricering te geven, zodat het gekoppeld kan worden met federatieve partners.

Het ontwikkelen en implementeren van een generiek koppelvlak is daarmee niet alleen een *silver bullet* om de balans te brengen, maar ook om de discussie over de balans met meer diepgang te bevorderen. De grote vraag blijft: hoe krijgen we onder alle omstandigheden en in ieder scenario de juiste informatie op tijd op de juiste plaats? Dit project geeft, samen met GrIT en het DEO, alvast een groot deel van het antwoord. En als we binnen dit project samen met gebruikers blijven pionieren en innoveren, dan zouden we zomaar onze *silver bullet* kunnen vinden!

Eindnoten

1 Dat ik als voormalig officier van de Geneeskundige Troepen een artikel mag schrijven in Intercom had ik nooit verwacht. Zeer vereerd, ik zal u mijn doopceel besparen, maar mocht het artikel leiden tot interesse neem dan gerust contact op met mij ad.colijn@mindef.nl of met de huidige projectleider van het project CDS.IV.444 Generiek Koppelvlak HGI AF.Veugelers@mindef.nl

2 Serendipiteit is het vinden van iets onverwachts en bruikbaars, terwijl de vinder op zoek was naar iets totaal anders.

3 Ballistic Missile Defense; Secure C2 Gateway; CDSIMS; Insight en C3PO.

4 Wat Defensie zelf levert wordt aangeduid met Government Furnished Equipment (GFE).

5 Er wordt voor het hardwarematig datafilter gebruik gemaakt van Field Programmable Gate Array technologie (FPGA).