HET DEFENSIE EXTRANET

FLEXIBEL SAMENWERKEN EN INFORMATIE DELEN MET PARTIJEN BUITEN DEFENSIE

Drs. A.A.D. (Barry) Dukker CISSP, Senior Innovatiemanager, DMO/JIVC/KIXS

Defensie moet meer en meer samenwerken en informatie delen met uiteenlopende partijen buiten Defensie. Denk hierbij bijvoorbeeld aan:

- Militaire missies en oefeningen met bondgenoten in NAVO- of EU-verband;
- Samenwerking met de industrie bij het ontwikkelen van wapensystemen;
- Wetenschappelijk onderzoek in samenwerking met kennis- en onderzoeksinstituten zoals de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO), het *Netherlands Aerospace Centre* (NLR), universiteiten en het bedrijfsleven;
- Samenwerking met ketenpartners in de Openbare Orde en Veiligheid (OOV), vreemdelingenketen, grensbewaking en de Kustwacht;
- Interdepartementale samenwerking en informatie-uitwisseling binnen de rijksoverheid;
- Studenten van hogere onderwijsinstellingen en de Nederlandse Defensie Academie (NLDA) die toegang moeten krijgen tot studievoorzieningen;
- Het uitbesteden van taken aan het bedrijfsleven, zoals bijvoorbeeld transport en logistiek. ➔

De lijst van partijen met wie Defensie moet samenwerken groeit gestaag. De behoefte om flexibel informatie met deze uiteenlopende partijen te kunnen delen wordt dus ook steeds groter. In dit artikel beschrijf ik eerst welke eigenschappen van de bestaande IT van Defensie maken dat de gewenste samenwerking momenteel problematisch is. Vervolgens beschrijf ik de stand van zaken van het project Extranet, dat hier een oplossing voor moet bieden.

Knelpunten bestaande IT

De MULAN-omgeving van Defensie en de talloze toepassingen die op MULAN worden aangeboden zijn van oudsher niet ontworpen om te worden gebruikt door medewerkers van externe organisaties. De huidige IT-omgeving en de toepassingen van Defensie zijn ontworpen om gebruikt te worden voor én door Defensiemedewerkers.
De MULAN-omgeving is opgezet als een gesloten bastion; een kasteel met een dikke buitenmuur en brede slotgracht gericht op het buitenhouden van buitenstaanders. Binnen de muren van het kasteel wordt iedereen vertrouwd, want alle gebruikers zijn per slot van rekening gescreend. Deze bastiongedachte is vanuit historisch perspectief verklaarbaar. Het is een afspiegeling van de manier waarop Defensie in het verleden dacht én werkte: eigen logistiek, eigen geestelijke verzorging, eigen geneeskundige dienst, eigen schoenmakers. Alles voor Defensie én vooral ook door Defensie.

Het bastionontwerp is echter niet geschikt voor het snel en flexibel samenwerken met onze ketenpartners, bondgenoten, kennisinstituten en de industrie. Als Defensie bijvoorbeeld een TNO-medewerker toegang wil geven tot één samenwerkingsruimte *(Sharepoint)* op het Defensienetwerk, dan wordt deze eerst geregistreerd in de personele basisadministratie. Vervolgens moet er een Verklaring van Geen Bezwaaar (VGB) worden afgegeven. Zodra aan deze basisvoorwaarden voldaan is, krijgt de TNO-medewerker een Defensiepas, een account op het netwerk, toegang tot de (virtuele) MULAN-werkplek, een e-mailbox van Defensie en (in potentie) toegang tot alle toepassingen op het Defensie intranet. Deze situatie is onwenselijk om een aantal redenen. De TNO-medewerker krijgt toegang tot véél meer toepassingen en informatie van Defensie dan hij strikt noodzakelijk nodig heeft, namelijk: die ene samenwerkingsruimte van het onderzoeksproject waaraan hij voor Defensie werkt. En naast het feit dat dit vanuit beveiligingsoogpunt onwenselijk is, is deze situatie ook niet financieel schaalbaar. Defensie maakt voor al deze externe personen te veel kosten, omdat het de enige manier is om een medewerker van een externe partnerorganisatie toegang te geven tot een samenwerkingsruimte op de MULAN-omgeving. Die kosten zouden nog te overzien zijn, als dit slechts enkele personen zou betreffen. Maar de behoefte om externe personen toegang te geven, neemt alleen maar toe, wat maakt dat de kosten voor Defensie hiermee evenredig oplopen.

“De TNO-medewerker krijgt toegang tot véél meer toepassingen en informatie van Defensie dan hij strikt noodzakelijk nodig heeft...”

Op het moment dat Defensie een specifieke toepassing wil ontsluiten naar een partnerorganisatie, dan doet zich nog een volgend probleem voor: de meeste toepassingen zijn qua informatiehuishouding ingericht op het bedienen van Defensiemedewerkers die voorkomen in de personele basisadministratie. Zo is het verstrekken van kleding door het Kleding en Persoonsgebonden Uitrustingsbedrijf (KPU-bedrijf) gekoppeld aan de informatie over de militair volgens de personele basisadministratie. Als het KPU-bedrijf naast militairen ook de uniformen van Politie en Brandweer zou moeten gaan leveren, dan moeten de systemen van het KPU-bedrijf zodanig worden aangepast dat de aanvraag- en uitgifteprocessen ook overweg kunnen met klanten die niet als militair in de personele basisadministratie van Defensie staan. Kortom: de bestaande IT-systemen van Defensie zijn van oudsher niet ontworpen om opengesteld te worden voor de partnerorganisaties met wie Defensie in toenemende mate moet samenwerken.

Het Defensie-Extranet

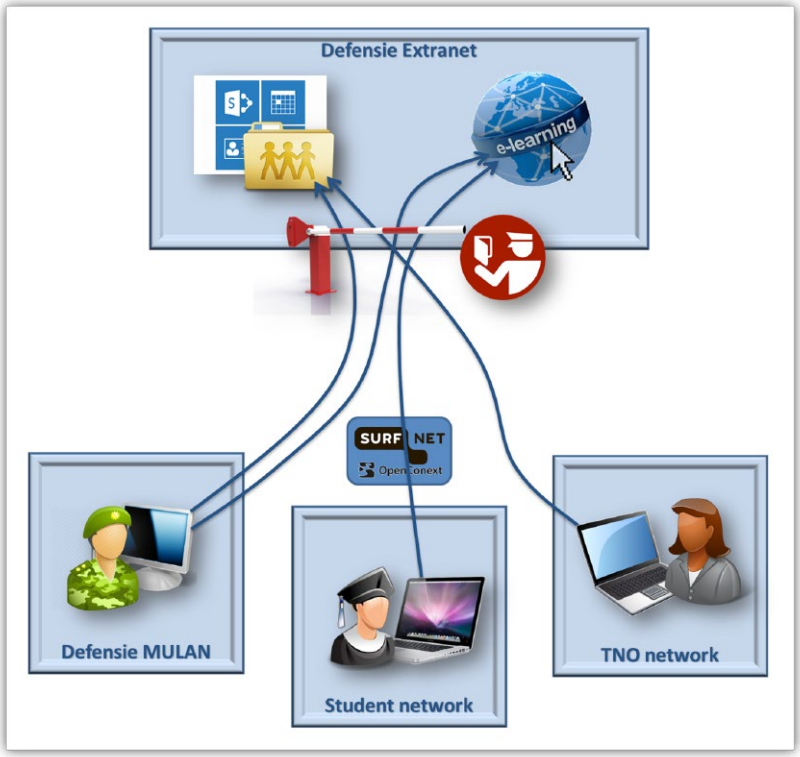
Om de behoefte aan samenwerking met partnerorganisaties op een snelle, flexibele én veilige manier te kunnen accommoderen, heeft de Directie Plannen van de Chef Defensie Staf

(CDS) begin 2014 een opdracht gegeven aan het Joint Informatievoorziening Commmando (JIVC) om een veilige extranetvoorziening te realiseren voor Defensie.
Het is daarbij expliciet de opdracht om een nieuwe, generieke voorziening te realiseren die geschikt is om in potentie alle verschillende samenwerkingsverbanden te kunnen bedienen. Het mocht expliciet geen specifieke *point solution* worden voor één specifieke casus.

De belangrijkste uitgangspunten voor het ontwerp waren:

- **Veiligheid:** de extranet beveiligingsarchitectuur moet het mogelijk maken op een verantwoorde wijze vertrouwelijke informatie te verwerken middels een omgeving waarop vertrouwde partnerorganisaties via het internet kunnen inloggen tot en met Departementaal Vertrouwelijk niveau.
- **Flexibiliteit:** de vele verschillende samenwerkingsverbanden waarin Defensie moet acteren hebben elk hun eigen set aan afspraken over de te gebruiken standaarden, protocollen en informatie-uitwisseling (technische en semantische interoperabiliteit).
  Het extranet moet zodanig van opzet zijn dat het overweg kan met al deze verschillende standaarden en afsprakenkaders op het koppelvlak naar de externe partnerorganisaties.
- **Toekomstvastheid:** de standaarden en protocollen op dit terrein zijn sterk in ontwikkeling. Defensie moet in staat zijn om de veranderingen in deze markt te kunnen volgen, zodat de interoperabiliteit met de partnerorganisaties ook naar de toekomst toe geborgd blijft.

De afgelopen jaren is er gewerkt aan de realisatie van een volledig nieuwe netwerkomgeving naast de bestaande MULAN-omgeving, gebaseerd op principes van federatieve samenwerking en ingericht op basis van een moderne beveiligingsarchitectuur. Deze nieuwe extranetomgeving is rechtstreeks benaderbaar voor Defensiemedewerkers vanuit de MULAN-omgeving en kan door een beveiligde koppeling met het internet ook benaderbaar gesteld worden voor medewerkers van vertrouwde partnerorganisaties. Het technisch ontwerp is in 2015 geïmplementeerd en in 2016 middels een *Proof of Concept* (PoC) beproefd. Nadat de technisch correcte werking van het systeem was aangetoond, is het project in 2016 gestart met de implementatie van de pilot-omgeving. Daar waar de technische PoC nog geen externe koppelingen naar het internet had, is de extranet pilot-omgeving wél benaderbaar via het internet.



De afgelopen periode is de veiligheid van de pilot-omgeving en de kwaliteit van de genomen beveiligingsmaatregelen aan de tand gevoeld door het *Defensie Computer Emergency Response Team* (DefCERT) dat een serie van zogenaamde penetratietesten op de extranet pilot-omgeving heeft uitgevoerd. Op basis van de resultaten van de penetratietesten door DefCERT zal de accreditatie van de extranet basisinfrastructuur worden aangevraagd bij de BeveiligingsAutoriteit (BA) van Defensie en kan de eerste externe koppeling naar een vertrouwde partnerorganisatie worden aangebracht.

De volgende stap

De eerste partnerorganisatie die op de pilot zal worden aangesloten is TNO. Nadat de toegang voor TNO-medewerkers via deze koppeling is gerealiseerd, zal het samenwerken op de samenwerkingsruimte van het extranet beproefd worden met echte eindgebruikers. Hierbij wordt in de pilot beproefd op welke manier de toegangsautorisaties voor verschillende medewerkers het beste ingericht en vormgegeven kunnen worden, inclusief de gevolgen van de afgestemde werkwijze voor het omgaan met de informatie en de toegangsregels binnen de samenwerkingsruimte.

Nadat ook de pilot met TNO succesvol is afgerond kan de extranet pilot-omgeving worden omgedoopt tot productieve dienstverlening en kunnen er meer toepassingen via de generieke extranet toegangsinfrastructuur aangeboden worden, mits deze toepassingen geschikt zijn voor gebruik door externe organisaties. Na jaren van voorbereiding, ontwerp, bouw en beproeving komt daarmee het einde van het project in zicht en is er een belangrijke nieuwe basis gelegd voor digitale samenwerking van Defensie met externe partners.