ZELF DOEN: BEVEILIGEN

Lkol Edwin Saiboo, hoofdredacteur

Mijn redactionele oproep aan de operationele gemeenschap heeft effect gehad. In deze Intercom ruime aandacht vanuit Eibergen en Garderen. Daarnaast ook innovatie in de nationale infrastructuur en vernieuwing en uitbreiding bij het Satelliet Grond Station in Lauwersmeer. Innoveren en vernieuwen is zo veel meer dan een symposium organiseren; vanuit de gedachte dat stilstand achteruitgang is en dat Defensie moet blijven vernieuwen om een operationeel voordeel te verkrijgen en te houden op onze opponenten. Waar die ook vandaan komen. Goed bezig!

De digitale werkplek van de toekomst en grenzeloze IT illustreren wat velen al weten: je hoeft niet alles zelf te ontwikkelen en te bouwen. Innoveren en beveiligen een sterke formule om het operationele voordeel te behouden. Omdat het moet. Het beheersen van de risico's kan echter niet worden genegeerd, het Bureau ICT Toetsing oordeelt over de nieuwe ICT van Defensie en schetst de zorgen.

Zorgen over aanpak nieuwe ICT Defensie

De plannen van het ministerie van Defensie voor een compleet nieuwe toekomstige IT-infrastructuur zijn risicovol. Dat concluderen onderzoekers die de plannen in opdracht van minister Jeanine Hennis-Plasschaert onder de loep hebben genomen. Hun rapport is begin juni gepubliceerd. Bepaalde risico's bij een programma als dit zijn onvermijdelijk. Ze waarschuwen voor de keuze van één hoofdaannemer voor het project. Dat kan tot hogere kosten leiden en het kan moeilijk worden om invloed uit te oefenen op de kwaliteit, omdat er geen concurrentie is. Verder bestaat de vrees dat er onvoldoende geld en kennis is om het project tot een goed einde te brengen. Het advies is bovendien om de plannen duidelijker te maken: ,,Er zijn vele wegen die naar Rome leiden, maar Defensie moet wel vooraf weten of ze via Brussel of Keulen reist, zodat ze een gerichte eerste stap kan zetten."

Risico's

Minister Hennis laat de Kamer weten dat 'terecht een aantal risico's zijn genoemd'. Volgens haar zijn 'bepaalde risico's bij een programma als dit onvermijdelijk'. Het komt er dan op aan om goed met die risico's om te gaan. D66-Kamerlid Salima Belhaj blijft kritisch: "Het Bureau ICT Toetsing oordeelt hard over de plannen van minister Hennis om de problemen met ICT grondig aan te pakken. ICT en Defensie zijn al heel lang geen goede combinatie en het lijkt erop dat de goedbedoelde plannen van de minister hier voorlopig geen verandering in gaan brengen." Wat je wel zelf moet blijven doen is beveiligen. Daar dus daar zeker niet alleen COTS, *commercial of the shelve*.

Ter illustratie een voorbeeld over e-mail die niet aankomt. 'En als er dan een *embedded* plaatje in zit denkt de firewall dat ik een virus wil inbrengen. Niemand krijgt daar bericht van om *security policy* redenen. De ontvanger niet en de zender ook niet. Volgens mij wel een dingetje om eens ter sprake te brengen. Je zou zomaar zeer belangrijke berichten van buiten kunnen missen. Waar is de quarantaine gebleven? Werd de bijlage geopend en ging de zaak alsnog door. Je zou ook zelf een foto kunnen maken (geautomatiseerd) van de bijlage en die intern versturen. Innovatie idee? De ontvanger kan het dan zien dat er iets voor hem is binnen gekomen. Je zou er ook een link van kunnen maken en de bijlage in een *sandbox* laten staan waar men via IODW (internet op de werkplek), naar kan kijken. Huidige situatie ken ik niet. Zal wel COTS zijn. En dan zijn we dus net zo (on)kwetsbaar als de rest van de COTS *community*. Defensie moet juist ook op dit vlak dingen doen die NIET COTS zijn.'
Zullen het dan toch weer de militairen en de burgers van Defensie zijn die het verschil maken? Omdat het moet, maar laat de '*can do* mentaliteit' niet onze ondergang worden. Veel (kritisch) leesplezier.