CYBERSECURITY EN RISICOMANAGEMENT

Ir. A.C.M. Smulders, TNO

Waarom is de huidige aanpak niet geschikt voor de problematiek van de toekomst? Dynamisch risicomanagement is een van de termen die met het opkomen van de aandacht voor cyberspace steeds prominenter naar voren komt. Dat er een noodzaak is voor dynamisch risicomanagement is eenvoudig te verklaren. De dynamiek van het cyberdomein is vele malen groter dan de dynamiek die we kennen in de fysieke wereld. Deze dynamiek wordt versterkt door behoefte aan flexibiliteit in samenwerkingsverbanden, snelheid van ontwikkelingen in het cyberdomein en toenemende vraag naar inter-connectie tussen informatiestromen, informatiesystemen en infrastructuren.

OVER DE AUTEUR

Ir. A.C.M. 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 naast programmaleider van het onderzoeksprogramma informatiebeveiliging voor defensie, ook trekker van het onderwerp cybersecurity binnen TNO. De auteur werkt aan diverse security en informatiebeveiligingsprojecten voor zowel Defensie als voor andere markten.

INTRODUCTIE

Huidige keten gebaseerde risico aanpak voldoet niet meer. Binnen het cyberdomein zijn twee tegengestelde trends waarneembaar die een grote invloed uitoefenen op de inrichting van risicomanagement. Aan de ene kant is er een toenemende opdeling van bestuurlijke verantwoordelijkheid. Waar in het verleden de verantwoordelijkheid voor alles wat noodzakelijk was voor het uitvoeren van een militaire missie in handen was van één verantwoordelijke binnen een hiërarchische lijn is de huidige praktijk dat men afhankelijk is van partijen (die opereren in toenemende dynamische samenwerkingsverbanden) die niet meer onder een hiërarchische verantwoordelijkheid vallen. Diezelfde ontwikkeling zien we in de infrastructuur die door het outsourcen van onderdelen niet langer meer onder de bestuurlijke verantwoordelijkheid van één partij vallen. Daarmee verdwijnt op bestuurlijk niveau langzaam de directe invloed en inzicht op hoe die onderdelen ingevuld worden. De trend is dat bestuurlijk gezien in toenemende mate wordt georganiseerd en gedacht in services die op het grensvlak van zo'n service aangestuurd wordt. Een service kan daarbij gezien worden als een black box, men is voornamelijk geïnteresseerd in de dienst zelf en niet hoe deze tot stand komt. Bestuurlijk gezien heeft het denken in services een aantal belangrijke voordelen. Kostenbesparing is daarin een belangrijke driver, bijvoorbeeld omdat men zelf niet meer de expertise in huis hoeft te hebben en doordat de aanbieder van de service zich daar in kan specialiseren en daarmee kosteneffectiever is.

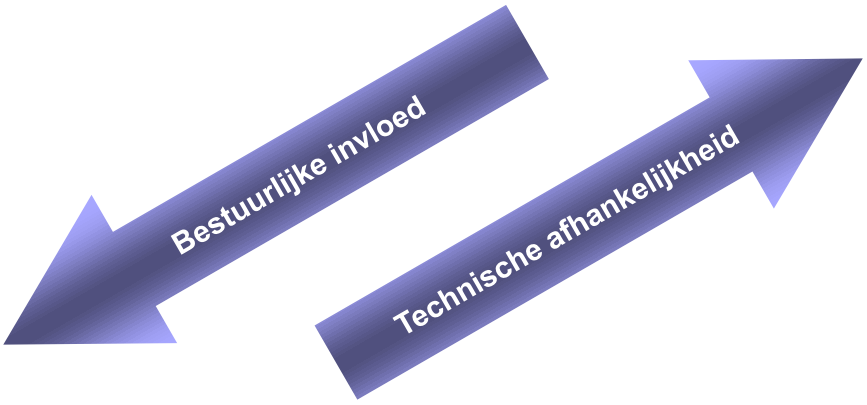
Aan de andere kant is een trend te zien dat het besef over de onderlinge technische afhankelijkheden tussen die verschillende onderdelen alleen maar toeneemt. Vanuit security technisch oogpunt is het daarom nog steeds gemeengoed om in ketens te denken. Dat is ook logisch omdat technisch gezien het in toenemende mate om technische ketens gaat.

Het opdelen van de bestuurlijke verantwoordelijkheid in de traditionele ketens staat haaks op de benadering vanuit de techniek om in ketens te blijven denken. Technisch worden de ketens steeds prominenter terwijl bestuurlijk die ketens steeds meer verdwijnen. Service georiënteerd denken en keten gericht risicomanagement gaan niet samen. Een toekomstgericht aanpak voor risico management is een aanpak die rekening houdt met deze twee tegengestelde ontwikkelingen.

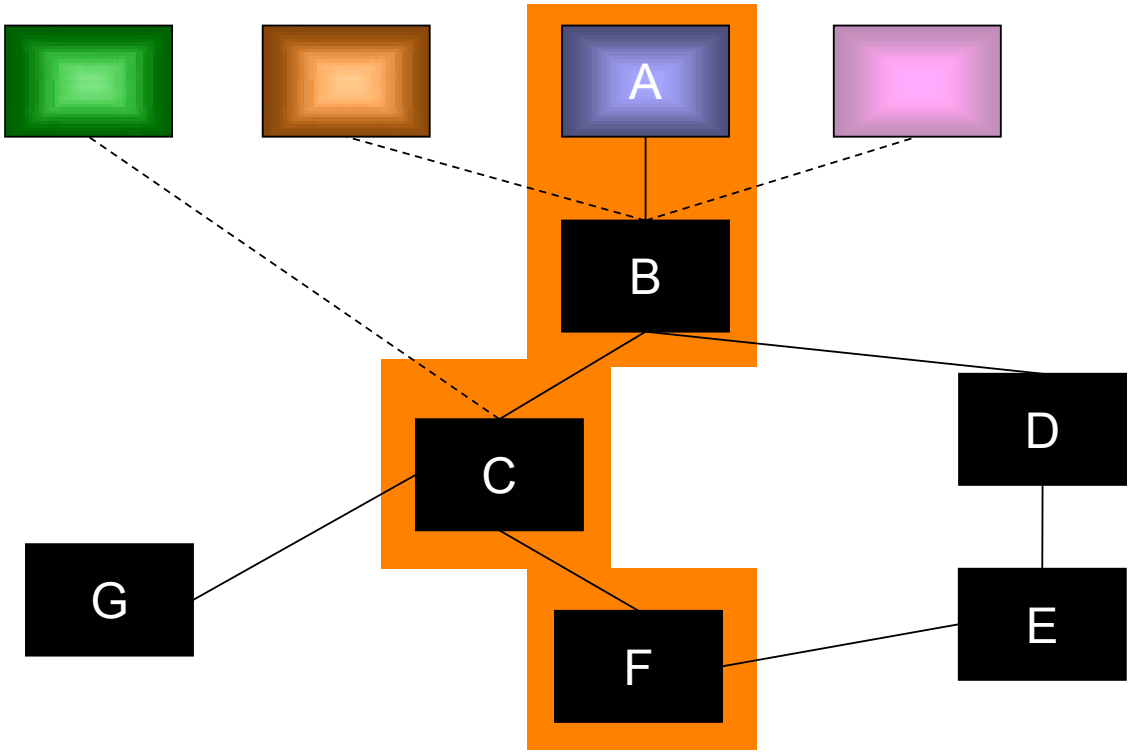
KETENS BESTAAN NIET MEER

Vanuit een technisch perspectief klopt deze uitspraak natuurlijk niet, omgevingen worden op technisch niveau in toenemende mate aan elkaar gekoppeld. Vanuit bestuurlijk perspectief is er echter niemand meer die eenduidig de verantwoordelijkheid over het geheel heeft. Binnen een organisatie misschien nog wel, maar zodra men buiten de organisatiegrenzen komt niet meer. Dat terwijl de technische afhankelijkheid niet ophoudt bij de eigen organisatiegrens. Daarbij komt dat door in toenemende mate op basis van services te denken en werken een web van services ontstaat die dusdanig complex kan worden dat het overzien daarvan niet of nauwelijks meer mogelijk is. Dit wordt versterkt doordat de services black boxes zijn waarvan de inrichting voor de gebruiker van die service niet meer inzichtelijk is.

Het gevolg daarvan is dat wat we traditioneel als keten zien, een projectie wordt op een web van services. Figuur 'Keten is een projectie op een web van services' laat dat zien.



Tegenstrijdige bewegingen.



Keten is een projectie op een web van services.

Met de inherente dynamiek in het cyberdomein kan deze projectie over een korte periode ook nog eens drastisch veranderen. Een dergelijk andere projectie is te zien in figuur 'Dynamiek is groter en minder inzichtelijk door complexiteit.

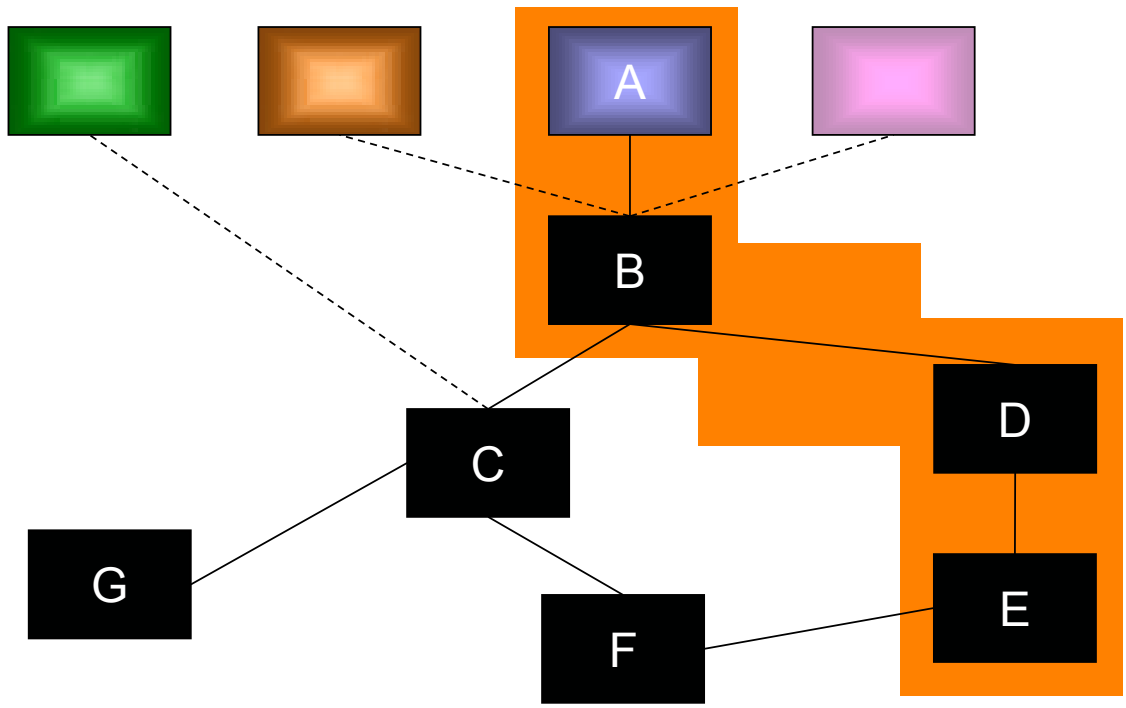
AANPAK VOOR DYNAMISCH RISICOMANAGEMENT

Een vanuit de techniek voor de hand liggende aanpak is om bestuurlijk weer de controle over de keten te nemen (bijvoorbeeld door te insourcen). We zijn echter al voorbij het kantelpunt dat dit een valide optie is. Een ander alternatief is om het ketendenken in risicomanagement los te laten en te zoeken naar een aanpak die gebaseerd is op services. De uitdaging die hierin voor security verborgen zit is de vraag hoe in deze situatie de assurance te borgen. Vaak wordt alleen gekeken naar de (security) eisen die door een service ingevuld dienen te worden. Voor functionele eisen is dat vaak eenvoudig vast te stellen, en is het antwoord op de vraag, levert een service een specifieke functie?

Voor de zekerheid dat die functie ook echt doet wat deze zou moeten doen conform gewenste eisen (*assurance*) is een stuk ingewikkelder. In de huidige risicomanagement aanpak wordt vaak teruggegrepen op een cristal box benadering waardoor inzicht te krijgen in hoe deze service is ingericht. Dit staat echter weer haaks op de bestuurlijke benadering waarin men hier geen invloed en/of inzicht meer in heeft.

De uitdaging voor een risicomanagement aanpak die waar nodig voldoende *assurance* kan bieden op basis van een black box methode. Geen makkelijke maar zeker ook geen onmogelijke opgave als men bedenkt dat toekomstig risicomanagement er vooral op gericht is om niet 100% zekerheid te bieden maar voldoende inzicht in actuele risico's op zodanige wijze dat een bestuurlijke verantwoordelijke (dat kan een beleidsmaker zijn, maar ook een operationeel commandant, en zelfs systeembeheerders) de juiste keuzes kunnen maken hoe met die risico's om te gaan.

TNO werkt aan dit concept en heeft een methodiek ontwikkeld die dit concept ondersteunt. Deze methodiek is in concept bij diverse (markt) partijen getoetst en lijkt een oplossing te bieden voor de hierboven benoemde tegenstrijdige bewegingen. De uitdaging voor defensie ligt in het onderzoeken of deze ontwikkelingen in de toekomst toepasbaar zijn binnen de defensie context.



Dynamiek is groter en minder inzichtelijk door complexiteit.