

## Platform Integrale Beveiliging (PIB)

*"Op het moment dat een aantal participanten het initiatief nemen om met elkaar te gaan praten over een mogelijke integratie van beveiligingsactiviteiten is in feite het eerste resultaat al binnen. Het geeft immers aan dat men bereid is om in breder perspectief te kijken naar mogelijkheden om gezamenlijke problemen aan te pakken".  
Mr Jan A. Seij; Vertas B.V.*

### Doelstelling

Het Platform Integrale Beveiliging beoogt een platform te zijn voor verschillende beveiligingsdisciplines; het fungeert als klankbord voor integratie-aspecten en het ontwikkelt initiatieven op het gebied van integrale beveiliging.

*Integraal* omdat het Platform openstaat voor alle security disciplines;  
geen afbakening vooraf.

*Beveiliging* omdat in eerste instantie beveiliging het vertrekpunt is;  
dat betekent niet dat geen aandacht wordt besteed aan veiligheid.

### Concreter

- Globaal inzicht in de verschillende beveiligingsdisciplines als het gaat om werkwijze en beschikbare, eventueel geautomatiseerde, hulpmiddelen
- Onderzoek naar integratie mogelijkheden
- Inzicht in kansen en valkuilen bij een integrale aanpak
- Opgedane kennis verspreiden

### Hoe te realiseren?

In werkgroepverband

- inzicht geven in verschillende benaderingswijze; bij voorkeur a.h.v. 1 casus
- integratie-mogelijkheden onderzoeken

PIB-bijeenkomsten

- podium voor verschillende integratie initiatieven; *informatief*
- resultaten werkgroepen presenteren; *klankbordfunctie*

Resultaten openbaar maken

- website
- publicaties
- presentaties tijdens beveiligingsevenementen

### Contactpersoon

Douwe P de Jong  
0653 789 245  
[jong.d@nvbi.nl](mailto:jong.d@nvbi.nl)  
Baanstraat 13 1135 CB

### Algemeen

Het Platform bestaat ruim 2 jaar; is 7 x bij elkaar geweest met tussen de 10 en 20 aanwezigen; de werkgroep bijeenkomsten zijn niet meegeteld. Ruim 40 personen hebben zich laten registreren als belangstellende.

### Organisatievorm

Het Platform is begonnen als een informeel groepje enthousiaste vakspecialisten en gastbedrijven faciliteren de bijeenkomsten. Toch is er behoefte aan meer 'body' om ideeën uit te werken en om een breder publiek te bereiken, zonder een nieuwe beveiligingsclub op te richten. Er zijn gesprekken geweest met de VBN om een vakgroep Integrale beveiliging & veiligheid op te richten. Hier is nog niets uitgekomen. Ook is een oproep gedaan om een landelijk evenement te organiseren: het PIB levert kennis, de andere partij het geld. Maar ook dat lijkt te blijven steken in aarzelende adhesie betuigingen.

### Wat kan het Platform betekenen voor beveiligingsland?

Er staan op dit moment 2 onderwerpen in de schijnwerpers die weerklank zou moeten vinden bij een bredere doelgroep.

Dat zijn *BORG & ICT* als integratie-initiatief aan de 'onderkant' van de beveiligingsmarkt en *Integrale beveiliging bij de overheid* aan de 'bovenkant' van de markt.

Daarnaast zijn de afgelopen periode diverse presentatie gehouden over grens overschrijdende beveiligingsproducten zoals een Digitaal Hekwerk, integratie van logische en fysieke toegangsbeveiliging en integrale security scans.

### BORG & ICT

De BORG-regelingen maken de fysieke beveiliging transparant voor zowel bedrijf en organisatie als voor de installateur. Binnen het Platform zijn intensieve discussies gevoerd hoe ook de informatietechnologie voldoende aandacht kan krijgen binnen de BORG-regeling. Uiteindelijk is de keus gevallen op een korte risico-afweging, gekoppeld aan maatregelklusters uit de Code voor Informatiebeveiliging. Bij het opstellen van het uiteindelijke beveiligingsplan moeten naast de BORG-maatregelcombinaties ook keuzes worden gemaakt voor de ict-maatregelklusters organisatie, voorschriften, logische toegang en continuïteit.

### Integrale beveiliging bij de overheid

Bij grote bedrijven en vooral met het in werking treden van het VIR ook bij de Nederlandse overheid, is een methodische aanpak van informatiebeveiliging gemeengoed; daarmee is ook de controlebaarheid van beveiligingsplannen en stuk eenvoudiger.

Voor fysieke beveiliging zag je tot voor kort wat aarzelende initiatieven. Daarin lijkt nu een doorbraak. Ook voor de fysieke beveiliging kan worden uitgegaan van een methodische aanpak zoals de A&K-analyse voorstaat en er zijn ontwikkelingen om dat geautomatiseerd te ondersteunen. Dit laatste niet met behulp van Cramm alhoewel er ook een initiatief is om CRAMM in te zetten voor fysieke beveiliging.

Kortom, initiatieven om fysieke beveiliging én informatiebeveiliging methodisch én controlebaar te benaderen.

### Hoe verder?

Als je echt iets wil bereiken heb je 'massa' nodig; een instituut met een breed draagvlak en met invloed in de maatschappij. Dat kan iets eenmaligs zijn, bijvoorbeeld aanschuiven aan een beveiligingsevenement. Of iets structureler door in een bestaande vereniging op te gaan met behoud van een eigen identiteit. En wellicht dat een landelijke presentatie daartoe nieuwe een impuls kan geven.

Integrale beveiliging beslaat een breed terrein; afhankelijk van het onderwerp bereik je een doelgroep.