



## Sector Overstijgend Security Overleg, deel 2

# Stap in een andere wereld

Security managers overleggen regelmatig over de problematiek binnen de eigen sector. Vaak komen hieruit bruikbare ideeën naar voren. Maar wat levert een overleg op waarbij vertegenwoordigers vanuit verschillende sectoren aanschuiven?

tekst Arjen Appelman

**N**a de introductie van het Sector Overstijgend Security Overleg (SOSO) in het april-nummer van Security Management is het tijd een eerste balans op te maken. Wat hebben de sectoren na een jaar van elkaar geleerd? En op welke onderdelen is aanvullend en verdiepend overleg noodzakelijk? Is het zo dat we kunnen stellen dat wanneer de ene sector een risicogebied ziet dat binnen haar sector nog onvoldoende aandacht heeft gekregen, het zo is dat we kunnen leren van een andere sector die hier wel al oplossingen voor heeft ontwikkeld? Het antwoord op deze vraag na een jaar SOSO is een voorzichtig ja.

## EÉN JAAR SOSO

Het eerste jaar heeft in het teken gestaan van de verkenning. Het gevoel te hebben telkens in een totaal nieuwe wereld te stappen is een onderdeel van deze verkenning. Maar ook het leren kennen van vakbroeders uit andere sectoren, het kennis nemen van elkaars ambities en overtuigingen is onderdeel van de verkenning geweest. En juist dit persoonlijke aspect bepaalt in grote mate de te behalen leereffecten. Daar waar we tijdens de eerste bijeenkomsten oppervlakkig met elkaar communiceerden, is geleidelijk een sfeer van vertrouwen ontstaan. Eigenlijk kunnen we stellen dat de laatste bijeenkomst, de evaluatie van een jaar SOSO, de meeste eye openers van het jaar met zich meebracht. Wat nodig is om van elkaar te kunnen leren, is een open sfeer van vertrouwen, een

omgeving waarin je je kwetsbaar kan en wilt opstellen. Daar liggen de kansen om rendement uit het sector overstijgende overleg te halen. En dat punt is na een jaar bereikt.

## LEERPUNTEN

Misschien is het grootste leerpunt wel het besef dat er een jaar nodig is om elkaar te leren kennen en vertrouwen. Pas nu kunnen we beginnen met het delen van dilemma's en op een ander niveau met elkaar in gesprek gaan. Het eerste jaar zijn leerpunten ontstaan door de sectoren met elkaar te vergelijken. Wat in de ene sector heel normaal is, kan in een andere sector totaal nieuw of ondenkbaar zijn. Daarom volgt nu een eerste beschouwing, waarin we een aantal sectorale vergelijkingen maken.

## RISICO'S

In de ene sector kan een risico geaccepteerd zijn, waardoor hier nauwelijks aandacht naar uitgaat (lees drugs aantreffen binnen een ziekenhuis bij een patiënt) terwijl dit binnen een andere sector het primaire aandachtspunt is (lees contrabanden aantreffen bij gedetineerden).

Interessant is ook om te horen dat risico's in verschillende tempo's veranderen. De risico's van het ziekenhuis en de Penitentiaire Instelling (PI) zijn redelijk stabiel, het risico van agressie in de zorg is al jaren bekend en verandert weinig behalve dan dat de ernst kan verschillen. Ook de zorg van het binnenbrengen



De deelnemers aan het eerste jaar SOSO (v.l.n.r.): Peter Sanders (PI Utrecht), Piet van Egmond (LUMC), Arjen Appelman, Raimond Pronk (Rotterdam The Hague Airport), Harm van Dijk (ING), André Delpeut (NRG).

van drugs en mobiele telefoons binnen een PI verandert wel maar niet heel snel. Echter, daar waar het gaat om airport security kan de dreiging van de ene op de andere dag totaal veranderen, moet je als beveiligiger de ene dag op scherpe voorwerpen letten, de andere dag kunnen daar vloeistoffen aan toegevoegd worden. De bank moet rekening houden met snel veranderende aanvalstechnieken op geldautomaten en telcentrales (denk aan explosieven, ramkraken, overval op geldlopers), waardoor beleid en voorzieningen behoorlijk aangepast moeten worden.

#### **BORGING BEVEILIGING EN INTEGRITEIT**

Verschillen zijn er ook voor de borging van beveiligingsprocessen. Zo zijn de processen binnen een academische omgeving en bij de overheid een stuk losser georganiseerd dan binnen een professionele zakelijke organisatie als een bank of een luchthaven. De wijze waarop medewerkers (Beveiliging) kunnen worden



#### **Vervolg SOSO...**



Inmiddels is het eerste jaar SOSO met de deelnemers geëvalueerd en is het overleg als interessant, zinvol en leuk betiteld. Afgesproken is in het vervolg verdieping te zoeken door in elke volgende bijeenkomst een dilemma van een van de aangesloten deelnemers uitgebreid met elkaar te bespreken. Een dilemma dat besproken kan worden is: hoe zorgen we ervoor onze voorzieningen op peil te houden tijdens bezuinigingen?

Naast de verdieping is het sectorale overleg met (vertegenwoordigers van) vier nieuwe sectoren uitgebreid. Het zijn allen kopstukken uit de retail, het openbaar vervoer, een multinational, en het cultureel erfgoed (museum). De eerste bijeenkomst staat inmiddels gepland.





aangesproken of aangepakt bij overtredingen zijn dienovereenkomstig. Doet een beveiligiger op de luchthaven iets dat tegen de regels ingaat, dan riskeert hij al snel ontslag op staande voet. Binnen de overheid betekent dit vaak in het ergste geval een aantekening in zijn of haar dossier. Bij de bank is security een onderdeel tijdens een functioneringsgesprek, bij het ziekenhuis is hiervoor nog een lange weg te gaan.

Omgaan met integriteit is een aanpalend onderwerp. Hiervoor moet binnen elke sector veel aandacht zijn, maar het verschilt in de praktijk behoorlijk. Worden er op de luchthaven en bij de kernreactor periodiek integriteitstrainingen georganiseerd binnen Beveiliging, bij het ziekenhuis en de PI moet hier veel meer aandacht aan besteed gaan worden. Denk als voorbeeld binnen de luchthaven na over het feit dat een medewerker Beveiliging een laagbetaalde baan heeft en hij dagelijks vele honderden koffers met luxe producten door zijn handen ziet gaan. Deze producten kunnen ze eenvoudig zien met de hypermoderne scanners die bedoeld zijn om gevaarlijke voorwerpen te detecteren.

#### INTEGRATIE BEVEILIGING EN VEILIGHEID



Die organisaties waar veiligheid letterlijk van levensbelang is - het academisch ziekenhuis en de PI - zien we dat beveiliging en veiligheid goed geïntegreerd zijn. Met name binnen deze organisaties levert het 24 uur in huis hebben van beveiligers die de organisatie op hun duimpje kennen grote voordelen op. De veiligheidsrisico's zijn binnen een grote bank met een paar duizend locaties veel gevarieerder. De grote hoofdkantoren waar duizenden mensen werken hebben dan ook een hele andere organisatie dan de vestigingen waar slechts een handvol mensen werkt. In de meeste vestigingen zijn helemaal geen beveiligers aanwezig en zijn deze taken belegd (wettelijk) bij de aanwezige bankemployees. Hoewel de integratiemogelijkheden niet overal gelijk zijn, is het toch interessant te zien dat er totaal verschillende organisatievormen mogelijk zijn. Het ziekenhuis en de PI hebben als primaire taak het voorbereid zijn op in- en externe rampen en calamiteiten getuige de SEH (spoedeisende hulp) van het ziekenhuis en het IBT (interne bijstandsteam) van de PI. Bij beide zijn er dagelijks spoedgevallen waar op uitgerukt moet worden. De getraindheid voor het onverwachte en de wijze waarop dit hier wordt onderhouden, is een mooi voorbeeld voor allen. Ook de luchthaven en de kernreactor kennen grote veiligheidsrisico's, waarvoor

## 'Om van elkaar te leren, is een open sfeer van vertrouwen nodig'

aparte, goed geoutilleerde brandweerkazernes zijn ingericht. Veiligheid en beveiliging zijn binnen deze organisaties ondergebracht in gescheiden organisatieonderdelen.

#### ORGANISATIE VAN BEVEILIGING

Naarmate de organisatie groter is, met als grootste organisatie de bank, is security meer opgeknipt in onderdelen. Daar waar de security manager verantwoordelijk is voor een onderdeel - de fysieke beveiliging - is binnen de kleinere organisaties de security manager verantwoordelijk voor meerdere disciplines. Hierbij is het wel zo dat informatiebeveiliging in bijna alle organisaties het domein is van een aparte functionaris, de security officer (bij de kernreactor is dit bij een persoon samengebracht). Ook verschilt de plek van de verantwoordelijke voor Beveiliging; binnen de PI is deze onderdeel van het management team van de instelling en valt een groot percentage van het totale FTE onder zijn hoede. Binnen het ziekenhuis is slechts een klein percentage van het totale aantal FTE beveiligers en behoren zij tot de facilitaire zaken. Alleen in het ziekenhuis en bij de PI zijn de beveiligers eigen mensen, bij de bank, de luchthaven en bij de kernreactor zijn het alle uitbestede diensten. Bij de luchthaven is dit wettelijk bepaald, de beveiligers mogen niet in dienst zijn van de luchthaven zelf. Daar waar het ziekenhuis en de PI niets liever hebben dan eigen medewerkers, willen de andere organisaties juist graag uitbesteden. Hier lijkt een relatie te liggen met de mate waarin beveiliging & veiligheid zijn geïntegreerd. ■

Arjen Appelman is directeur van Aes Security Management