

Integrale veiligheid

FM ALS DÉ REGISSEUR VAN VEILIGHEID



In veel organisaties is de verantwoordelijkheid voor (delen van) veiligheid op verschillende niveaus of afdelingen belegd. Dat kan goed werken, maar het kan om verschillende redenen ook leiden tot zwakke plekken in het beveiligingsconcept. Voor een integrale aanpak is het beter om de regie bij één centrale afdeling te leggen. FM is bij uitstek geschikt om die regisseursrol te vervullen.

DOOR FRANS VISSER EN LIES THURING*

In steeds meer organisaties is er het besef dat bij het realiseren van een veilige werkomgeving vandaag de dag een diversiteit aan onderwerpen speelt. Het gaat namelijk niet meer alleen om fysieke beveiliging, maar ook om zaken als bedrijfshulpverlening, informatiebeveiliging, crisismanagement en business continuity management.

Meestal wordt de verantwoordelijkheid voor die onderwerpen op verschillende niveaus en/of afdelingen belegd. Hieronder een voorbeeld van een dergelijke organisatorische verdeling:

- > FM = Fysieke beveiliging
- > HRM = BHV
- > ORM = non-financial Risico analyses & audits
- > IT = Informatiebeveiliging en IT-security
- > IT of een andere willekeurige afdeling = BCM (Business Continuity Management).

Een dergelijke verdeling is logisch en biedt een aantal voordelen. Tegelijk kan het ook minder positief uitpakken en nadelige gevolgen hebben. Denk bijvoorbeeld aan versnippering van kennis, het mogelijk ontstaan van competentieverschillen, het risico dat dubbel werk wordt uitgevoerd en de kans dat er geen of weinig samenwerking tussen de desbetreffende afdelingen tot stand komt. Dat is jammer, want juist die onderlinge afstemming en samenwerking zijn voor een organisatie cruciaal om haar 'kapitaal' (= medewerkers, gebouwen, inventaris, informatie) optimaal te beschermen.

SAMENHANG

Om te zorgen voor een veilige organisatie, zijn vier stappen te onderscheiden.

1. **Awareness:** het aantonen dan wel het besef van 'sense of urgency' om veiligheid actief en integraal te benaderen.
2. **Preventie:** het organiseren van bescherming van mensen, gebouwen, informatie en goede-

ren tegen mogelijk onheil. Door middel van een of meerdere risicoanalyses is bepaald tegen welke onheil (bijvoorbeeld; brand, overval, insluiping, fraude, maar ook mogelijke bedrijfsongelukken zoals uitglijden en vallen) preventieve maatregelen getroffen moeten worden.

3. **Repressie:** als toch een incident plaatsvindt, moet een reactie volgen. Voorbeeld: bij een bedrijfsongeval zal de BHV optreden, bij een inbraak komt de beveiligingsdienst in actie. Mocht het incident te groot van omvang zijn (geworden) voor de lokale organisatie, dan wordt de crisismanagement organisatie ingeschakeld en wordt de crisis vanuit een centrale organisatie aangepakt. Op enig moment tijdens iedere crisis rijst de vraag hoe nu morgen verder met de bedrijfsvoering en/of productie. Mocht een crisis langer aanhouden, dan is het tijd om de vooraf geanalyseerde, georganiseerde en getrainde BCM organisatie in te schakelen. Het organiseren van (tijdelijke) uitwijk van mensen, systemen en middelen is dan aan de orde om de continuïteit van de organisatie te waarborgen.

4. **Recovery:** in de fase 'recovery' is het doel om vanuit de crisis en/of de uitwijksituatie weer zo snel als mogelijk terug te keren naar de normale bedrijfsvoering. De BCM-organisatie draagt hier zorg voor. Na afronding kan de BCM- en crisisorganisatie zichzelf afschalen.

DOEL VAN INTEGRALE BENADERING

Het is niet de insteek van dit artikel om een pleidooi te houden om alle veiligheidsonderwerpen hiërarchisch bij één afdeling onder te brengen. Sterker nog, concentratie van alle veiligheidsonderwerpen op één afdeling kan juist averechts werken omdat het kan leiden tot te weinig draagvlak binnen de organisatie voor het geformuleerde veiligheidsbeleid en de getroffen veiligheidsmaatregelen.

Het is juist zinvol voor een organisatie om, daar

>>

Verantwoordelijkheden verdelen is logisch, maar kan nadelige gevolgen hebben.

waar de kennis en deskundigheid structureel aanwezig zijn, ook het betreffende veiligheidsonderwerp te beleggen. Maar omdat ieder veiligheidsonderwerp deel uitmaakt van de complete 'veiligheidspuzzel', is het van belang om één centraal punt binnen de organisatie te belasten met de coördinatie en onderlinge afstemming.

Vanuit zo'n centraal punt kan beleid op elkaar worden afgestemd, kunnen overlappen worden gesignaleerd en voorkomen, kan het trainen en opleiden van medewerkers worden georganiseerd enzovoort.

LOGISCHE STAP

Juist hier liggen kansen voor FM. Waarom FM? FM is vaak al intensief betrokken bij de uitvoering van de preventie, repressie en recoverystappen van het veiligheidsgebied. Het is voor de facilitaire afdeling dus een logische stap om als 'spelverdeler' en regisseur van integrale veiligheid te fungeren en op die manier de verbinding tussen 'strategie' en 'operatie' te leggen. Zo'n regisseur draagt zorg voor organisatiebrede afstemming van de veiligheidsbeleidsgebieden, voert risicoanalyses uit, coördineert interne- en externe audits et cetera. Daarnaast is FM als de regisseur hét centrale aanspreekpunt voor de directie met betrekking tot de veiligheidsonderwerpen die spelen.

LUST OF LAST?

FM als regisseur van integrale veiligheid biedt de organisatie voordelen. Met een interne centrale regisseur heeft het management bij vragen een direct aanspreekpunt. Ook voor interne- en exter-

MET DE REGISSEURSROL KAN FM HAAR MEERWAARDE VOOR DE ORGANISATIE NOG MEER AANTOONBAAR MAKEN

ne toezichhouders en bijvoorbeeld normeringsinstituten biedt deze organisatie een duidelijk 'anker' om binnen organisaties de 'weg' te vinden. Daarnaast biedt de regisseursrol FM een kans om haar meerwaarde voor de organisatie nog meer aantoonbaar te maken.

Om als FM deze regisseursrol succesvol te kunnen uitvoeren, is het wel zaak dat de afdeling beschikt over de juiste kennis, deskundigheid én senioriteit. Met kennis en deskundigheid wordt niet bedoeld dat FM moet concurreren met de gespecialiseerde afdelingen binnen de organisatie, maar dat de afdeling bij veiligheidsissues als projectmanager het voortouw neemt om de veiligheidsspecialisten te coachen, te stimuleren, te informeren, aan te vullen en beter te laten samenwerken. Dit alles om ervoor te zorgen dat het uiteindelijk doel - zorgdragen voor een veilige werkomgeving waardoor het primair proces optimaal kan functioneren - kan worden behaald. <<

DE 7 STAPPEN VOOR INTEGRALE VEILIGHEID BINNEN EEN ORGANISATIE

1. Awareness en 'sense of urgency' bepalen
2. Risicoprofiel van de organisatie ontwikkelen
3. Inventarisatie en bepalen van de 'key assets'
4. Bepalen van de preventieve risicostrategieën
5. Treffen van preventieve maatregelen
6. Implementatie van crisis en Business Continuity Management
7. Het proces cyclisch en innovatief maken



*Frans Visser en Lies Thuring zijn verbonden aan Visser & Van der Ven, security management.