

Groeien in security performance management

Security *performance* management is een hulpmiddel voor het management in grote organisaties om de securityfunctie aan te sturen en te verbeteren. Dit gebeurt door van de belangrijkste prestatie-indicatoren informatie te verzamelen, deze te veredelen en in een geëigende rapportagevorm te communiceren. Ofschoon voor diverse gebieden *performance* management wordt toegepast, is dat binnen security nog relatief nieuw. In een serie van twee artikelen worden de kenmerken van security *performance* management verkend. JORIS HUTTER *

Dit eerste artikel plaatst security *performance* management in een context en geeft aan waarop gelet moet worden bij het kiezen van prestatiekenmerken. Ook wordt aangegeven hoe de managementinformatie gebaseerd op deze prestatiekenmerken gemaakt kan worden. De managementinformatie moet tot verbeteracties leiden. Daarover gaat het tweede artikel. In dat artikel zal ook een aanpak worden beschreven om via volwassenheidsniveaus te groeien in security *performance*.

Security binnen grote organisatie

Voor iedere grote organisatie is het definiëren, vasthouden en aanpassen van de securityfunctie een lastige zaak. De meest complexe organisatievorm is die van een concern met vele vestigingslocaties. Op locatieniveau spelen de lokale risico's en in internationaal verband ook nog de daar geldende regelgeving en businesspraktijken. Wat beschermd moet worden en in welke mate, is sterk afhankelijk van het type bedrijfsproces en de businessunit van de locatie. Ten slotte moet op lokaal niveau ook rekening gehouden worden met het *corporate* beleid, omdat de lokale risicobeheersing ook een uitwerking kan hebben op andere delen van het concern.

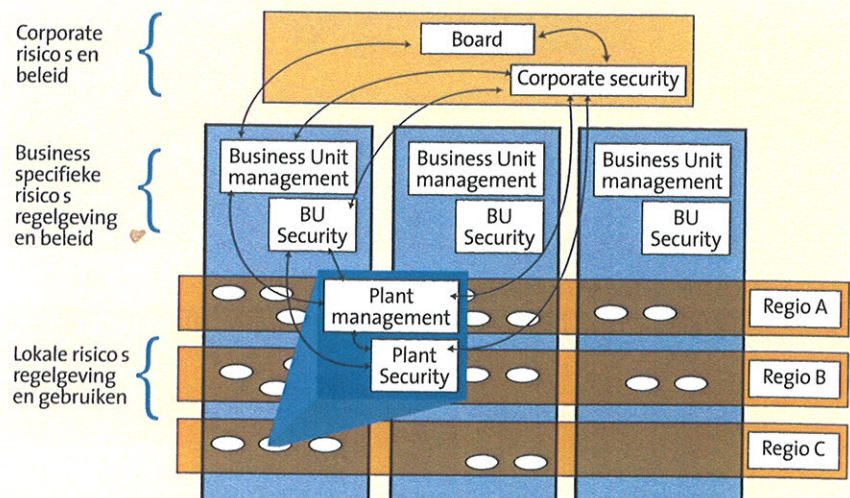
De eindverantwoordelijkheid voor security is in de lijn verankerd in een in-

tegrale managementfunctie. Op lokaal niveau is er vaak een *plant* security manager aanwezig als coördinatiepunt voor de security. Veelal is dat geen securityexpert, maar een functionaris die dit als deeltaak heeft. Op *corporate* niveau bevindt zich de *corporate* security manager, met soms een kleine staf van experts. De taak van deze manager is primair die van assistentie naar de *board* in de definiëring en handhaving van een *corporate* securitybeleid. Dit gebeurt natuurlijk in samenhang met andere stafafdelingen zoals HRM, ICT, Health, Safety en Environment. Daarnaast kan de *corporate* securitystaf specialistische expertisediensten leveren aan de businessunits en locaties. Om lijn en synergie in de security te krijgen kunnen er organisatorische richtlijnen gelden voor meerdere of alle vestigingen, kan er gebruik worden gemaakt van uniforme toegangssystemen en andere securitysystemen en

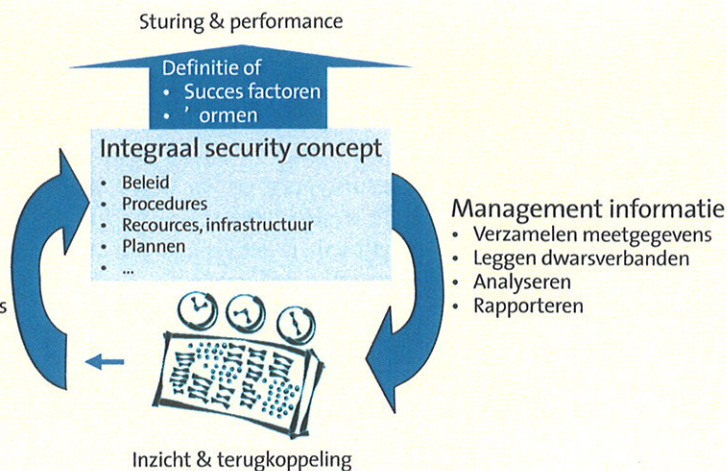
zullen mogelijk beveiligingstaken uitbesteed zijn die effect hebben op verschillende businessunits. Daarnaast worden natuurlijk diverse securitydeeltaken uitgevoerd door andere stafdiensten zoals ICT en HRM.

Het regie voeren over de risicobeheersing in een dergelijke organisatie is lastig. Hoe is duidelijk of de securityrisico's voldoende zijn afgedekt? Waaruit bestaat de security en hoe is helder of de maatregelen worden toegepast en functioneren? Hoe kan meer gehaald worden uit de dienstverlening van de security *service providers* en uit de securitysystemen? Hoe zijn de betrokkenen in het management en de beveiligingsorganisatie en zijn eindgebruikers te richten op de meest belangrijke securitydoelen? Hoe is duidelijk of de beveiligingsfunctie aangepast moet worden en in welke zin verbeterd dient te worden?

Naast organisatorische complexiteit zijn er vaak ook andere oorzaken aan



- Verbeteren**
- Organisatie & verantwoordelijkheden
 - Verantwoordingproces
 - Sturen op tijd en resources
 - Motiveren
 - Verbeteren
 - Verschil maken tussen gemiddeld en uitstekend



te wijzen voor een te geringe aandacht voor continue verbetering van de securityprestatie:

- » gebrek aan inzicht in de knelpunten en mogelijke verbeteringen;
- » afstand tussen de securityprestatie en de businessprestatiekenmerken;
- » tijdgebrek en beperkte capaciteit van securityspecialisten;
- » gebrek aan financiële middelen voor structurele investeringen;
- » sterke kortetermijnfocus en incidentgedreven inrichting van de beveiliging.

Meten is weten

Security *performance* management is voor de manager een instrument om op basis van goede informatievoorziening de securityfunctie te kunnen aansturen. Dit gebeurt naast andere hulpmiddelen als bijvoorbeeld het auditprogramma.

Sommige organisaties kennen al een *performance* managementsysteem. In dat geval kan de security-aanpak hierop aansluiten en verbijzonderen. Het INK-model (Instituut Nederlandse Kwaliteit) en de *Business Balanced Scorecard* (Kaplan en Norton) zijn voor velen bekende begrippen.

Ofschoon het securityvakgebied veel kan leren van de theorie en praktijk van *performance* management, zijn heel wat modellen nogal complex en te weinig afgestemd op het gebruik door de security manager. In dit artikel wordt de kern van *performance* management teruggebracht tot drie samenhangende processen:

1. het definiëren van de prestatiekenmerken van de security;
2. het verzorgen van managementinformatie op deze kenmerken;
3. het ondernemen van actie bij personen en partijen die de security kunnen beïnvloeden.

Deze drie processen moeten in samenhang en op gelijkwaardig niveau ingericht en uitgevoerd worden. Het heeft bijvoorbeeld geen zin om de securityinformatie verder te verbeteren als de prestatie-eisen niet helder zijn of als de organisatie niet rijp is om verbeteringen door te voeren.

Definiëren prestatiekenmerken

Zonder *performance* management blijven de securitydoelstellingen vaag en dubbelzinnig. Door gebrek aan inzicht in die securityaspecten die er echt toe-doen, is er ook weinig lijn en excellentie in het ontwerp en in de uitvoering van de security. Er is een verspilling van menstijd en middelen en de securityfunctie als geheel is onvoldoende geloofwaardig naar de betrokken partijen. Start met het definiëren van de security-succesfactoren die te maken hebben met de *stakeholder*relaties. Deze succesfactoren vormen de legitimatie van de securityfunctie en dus ook de kern van de security *business case*. In ruil voor

een bijdrage van de securityfunctie aan de *stakeholder*belangen, mag de security ook wat terugverwachten van deze *stakeholder*. Op beide relaties moeten in de concrete situatie de succesfactoren worden vastgesteld en verbijzonderd naar normen waarop gerapporteerd, gecommuniceerd en gestuurd kan worden.

Naast deze legitimatiedoelstellingen van de security zijn er ook andere succesfactoren die in meer of mindere mate van belang zijn voor de concrete inrichting en uitvoering van de security:

- » Snelheid van reactie- en aanpassingsvermogen. Dit is het vermogen van de organisatie om snel te kunnen schakelen naar andere securityniveaus, om snel in te spelen op specifieke securitydreigingen en in zijn algemeenheid om de securityfunctie te innoveren op wijzigingen van *stakeholder*behoeften, securitytechnologie en beschikbare inzichten.
- » Voortgang van projecten. Binnen veel organisaties zijn programma's »

Stakeholder	Bijdrage security aan stakeholder	Contributie stakeholder aan security en organisatie
Board, investeerders, banken, toezichthouder	<ul style="list-style-type: none"> • Heldere risico's • Kostenefficiënte risicobeheersing 	<ul style="list-style-type: none"> • Deelnemen aan risico's • Investeren
Klanten en schakels naar eindklant	<ul style="list-style-type: none"> • Veilige, prettige koopomgeving • Betrouwbaarheid product, dienst • Betrouwbaarheid leveringsproces 	<ul style="list-style-type: none"> • Hogere prijs • Loyaliteit
Medewerkers en vakbonden	<ul style="list-style-type: none"> • Veilige werkomgeving (fysiek en integer) 	<ul style="list-style-type: none"> • Betrokkenheid bij risicobeheersing • Betrokkenheid bij bedrijf (inzet, ziekteverzuim)
Leveranciers, contractors	<ul style="list-style-type: none"> • Betrouwbare klant 	<ul style="list-style-type: none"> • Betrokkenheid bij risicobeheersing • Betrouwbaarheid leveringsproces
Regelgevers, actiegroepen, communicatie	<ul style="list-style-type: none"> • Voldoen aan regelgeving • Veilige buurman 	<ul style="list-style-type: none"> • Rekening houden met business-eisen bij regelgeving • Actieve inzet op veiligheid bedrijf

gedefinieerd om securitymaatregelen in te voeren. Een bekende succesfactor van de securityfunctie is het vermogen om deze projecten ook daadwerkelijk uit te voeren.

- » Beheer. Hierbij ligt de succesfactor in het aantoonbaar maken dat gedefinieerde en geïmplementeerde beveiligingsmaatregelen ook daadwerkelijk aanwezig zijn en functioneren. Het periodiek inspectieprogramma van DHM is hier een voorbeeld van.
- » Kennis van risicobeheersing. Bewustwording, competenties en betrokkenheid vormen een van de pilaren van een effectief security-beleid. Om hierop te kunnen sturen, zullen ook prestatiekenmerken vastgesteld moeten worden. Een prestatiedoel kan zijn dat op een locatie 90 procent van het personeel moet weten op welke wijze onregelmatigheden moeten worden gemeld. Een ander prestatiedoel kan zijn dat minimaal vier keer per jaar in het werkoverleg over security moet worden gesproken.
- » Oorzaak en gevolg. Het inzicht in knelpunten en in oplossingen wordt enorm vergroot als er oorzaak-en-gevolgrelaties gelegd kunnen worden. Een voorbeeld is het aantal incidenten op een locatie in relatie tot het falen van het toegangsbeleid. Moet het toegangsbeleid correct of aangescherpt worden uitgevoerd of moeten er andere maatregelen getroffen worden om de incidenten te voorkomen?
- » *Level of effort*. Dit zijn prestatiekenmerken die aangeven hoe efficiënt routinetaken worden uitgevoerd. Bijvoorbeeld: snelheid en kosten van het maken van een toegangspas.

Managementinformatie

Zonder *performance* management is er

Kwaliteit van meetpunt

Neely hanteert de volgende testen om de kwaliteit van een meetpunt te bepalen en te verbeteren.

1. Waarheid - meten we echt wat we overeengekomen zijn te meten?
2. Focus - meten we alleen datgene wat we hebben besloten te meten?
3. Relevantie - is het de juiste maatregel van de performance factor die we willen volgen?
4. Consistentie - worden alle data op dezelfde wijze verzameld?
5. Verkrijgbaarheid - is het eenvoudig deze data te verzamelen?
6. Klarheid - is het mogelijk dat data verkeerd geïnterpreteerd worden?
7. Inzicht - kan op de juiste manier actie worden genomen op de verkregen data?
8. Tijdigheid - kunnen de data snel en frequent verkregen worden om actie te nemen?
9. Kosten - is de maatregel het waard om gemeten te worden?
10. Ongewenst spel - is het mogelijk dat de maatregel aanmoedigt tot ongewenst gedrag?

geen goede informatie over de securityfunctie, zal er alleen op onderbuikgevoel gestuurd kunnen worden en ontbreekt een heldere onderbouwing waarom bepaalde maatregelen gewenst zijn. Ook bij het ondoordacht opzetten van managementinformatie kan de situatie ontstaan dat de rapportages veel ruis bevatten, maar niet gaan over de kritische succesfactoren van de security.

Een belangrijk kenmerk van *performance* managementinformatie is dat deze normatief is en vergelijkbaar. De vergelijking op beveiligingsprestaties kan binnen de organisatie liggen, maar kan ook een *benchmark* zijn met externe, vergelijkbare organisaties. Ook kan de ontwikkeling van de securityprestatie in de tijd worden gevolgd en vergeleken. Ten slotte kan de prestatie ook vergeleken worden met een door de organisatie zelf gedefinieerde norm. De selectie van meetpunten vraagt veel aandacht. Zie de tien kwaliteitsvragen van Neely om de kwaliteit van een meetpunt te bepalen. Met het groeien in security *performance* management, kunnen meetpunten ook gewijzigd worden naar sterkere indicatoren. De wijze van presenteren is afgestemd op de gebruikseisen en -wensen. Dat kan een mondelinge presentatie zijn, maar zal natuurlijk vaker een getals-

matige of een visuele presentatie zijn. Naast kwaliteit van de brongegevens is de ict-tooling van belang. Hierbij zijn verschillende valkuilen. Een *performance* traject kan snel opgestart worden als de gegevens handmatig worden verzameld en worden gepresenteerd in een Microsoft-Excel-achtige omgeving. Als het aantal rapportages groeit, wordt deze werkwijze onbeheersbaar en is de rapportage niet meer aanpasbaar aan nieuwe wensen. Op een gegeven moment zal overgestapt moeten worden naar een meer volwassen en geïntegreerd proces met een *business intelligence tool* om de gegevens te verzamelen, te analyseren en te presenteren. In ultieme vorm kan dat een dashboard zijn waarin indicatoren in kleur aangeven of er actie gewenst is en waarin de gebruiker via 'drill down' achtige technieken de brongegevens kan analyseren. Daarbij moet er op worden gelet dat het een *performance* project blijft en geen it-project wordt.

Vervolg

Dit eerste artikel beschreef de factoren om de prestatiekenmerken op de security te definiëren en om tot managementinformatie te komen. Het gaat er natuurlijk om dat er gehandeld wordt. In het tweede artikel wordt aandacht besteed aan de factoren om op basis van de managementinformatie tot effectieve verbeteracties te komen bij al die personen en partijen die invloed hebben op de security. Tevens bevat dat artikel een bruikbare aanpak om via volwassenheidsniveaus te groeien in security *performance*. «

* Drs. Joris Hutter RSE RCE, Hutter Security Risk Management

Samenvatting

- » Security *performance* management is een **hulpmiddel** voor het management in grote organisaties om de securityfunctie aan te sturen en te verbeteren.
- » Het is van belang security *performance* management in de juiste **context** te plaatsen en **succesfactoren** en **prestatiekenmerken** te definiëren.
- » Het maken van **managementinformatie** op basis van deze prestatiekenmerken is vervolgens essentieel.

De succesfactoren voor management

Security performance management is een hulpmiddel voor het management in grote organisaties om de securityfunctie aan te sturen en te verbeteren. Binnen security is dat nog relatief nieuw. In deel 1 in *Security Management* nr. 5 werd de kern van performance management teruggebracht tot drie samenhangende processen. In dit slotartikel wordt ingegaan op het definiëren van de succesfactoren en het opstellen van managementinformatie. JORIS HUTTER *

Bij security performance management gaat het er om dat er wordt gehandeld. Dit tweede artikel gaat dan ook over factoren die van belang zijn om tot effectieve verbeteracties te komen bij alle personen en partijen die invloed hebben op de security. Daarna wordt aandacht besteed aan een volwassenheidsmodel dat bruikbaar kan zijn bij het groeien in security performance.

Sturen is de kunst

Er kunnen verschillende oorzaken zijn dat personen en partijen die invloed hebben op de security deze niet effectief aanwenden. Dat is het geval als de organisatie van de beveiliging onduidelijk is en als de verantwoordelijkheden vaag zijn gedefinieerd. Het ontwerpen en invoeren van een helder organisatie-model met bijbehorende verantwoordelijkheden is daarom essentieel om te kunnen sturen.

Maar ook de cultuur is van belang. Als deze zodanig is dat personen hun verantwoordelijkheid ontlopen, kan er ook niet geïnnoveerd worden en zal eerst aan een duidelijk verantwoordingsproces moeten worden gewerkt. Tevens kunnen persoonlijke carrières een verbetering van de security in de weg staan. Dit gevaar moet worden onderkend en het moet helder worden gemaakt dat security performance manage-

ment alleen bedoeld is om de security aan te sturen en te verbeteren en niet als afrekenmodel voor betrokkenen. Evenzo is er een balans tussen de vrijheid c.q. strakheid waarin de prestatienormen worden gesteld. Als de prestatienormen te weinig ruimte overlaten voor een eigen werkmethode, kan dat demotiverend en averechts werken. Omgekeerd kan een te grote vrijheid voor een eigen werkaanpak vergelijkingen en verbeteringen onmogelijk maken.

Verantwoording is het actief onderhouden van een relatie tussen partijen. Het is resultaatgericht. Security performance management is in dit verantwoordingsproces een goed instrument, omdat het zowel de resultaatgebieden omvat als de rapportage hierop. In het definiëren van rapportages en van verantwoordingsprocessen kan onderscheid worden gemaakt naar een individuele verantwoording waarbij de verantwoordingsrelatie op taakniveau ligt in de eigen werkomgeving, een teamverantwoording waarbij er een gedeelde verantwoordingsrelatie is vanuit het team, of een organisatieverantwoording naar interne of externe partijen. De regelmatige terugkoppeling op de prestatiedoelstellingen kan motiverend zijn en vormt de kortste weg om doelstellingen te bereiken. De besluitvorming op de inrichting en

budgetten van security wordt ondersteund door objectieve informatie over en inzicht in de security. De managementinformatie is een van de bronnen voor dit inzicht. Dit inzicht wordt ook gevormd door aanvullend onderzoek door de securitystaf. De managementinformatie is dan tevens een hulpmiddel om deze beperkt beschikbare securitystaf zo gericht mogelijk in te zetten op die locaties en issues die de meeste support nodig hebben.

Groeien in performance

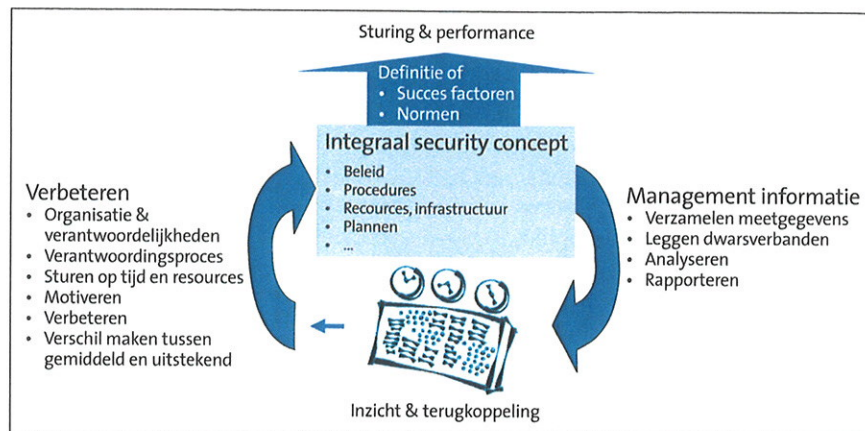
Wij introduceren nu het concept van volwassenheidsniveaus. Voor de eenvoud hanteren wij er drie. Daarbij is het idee dat het securityconcept en de onderdelen van de performance managementaanpak in balans op een bepaald niveau aanwezig moeten zijn, voordat het zinvol is om te groeien naar een hoger niveau.

In de startfase dienen de verschillende onderdelen te worden gekwalificeerd. Als er discrepanties zijn in het niveau zal eerst aandacht moeten worden besteed aan de onderdelen die nog onvoldoende ontwikkeld zijn. Het opstellen van een volwassenheidsmodel is altijd arbitrair. Toch is het van belang om helder te maken hoe een organisatie systematisch en effectief kan groeien in haar securityprestatie.

security performance

Basisniveau

Op het basisniveau is het integrale securityconcept nog niet of slechts beperkt gedefinieerd. Op doelstellingen-niveau is het zinvol om de *business case* van security helder te maken. Zoals in het eerste artikel is aangegeven, wordt die verbijzonderd door de securityprestatiekenmerken op de relaties met de stakeholders. Deze kenmerken zijn namelijk ook nodig voor het verdere ontwerp van het integrale securityconcept. Een andere doelstelling is om het implementatieproces van securitymaatregelen goed te kunnen volgen. De informatievoorziening kan in deze fase eenvoudig zijn, omdat alleen de projectvoortgang en een beperkt aantal prestatiekenmerken op de stakeholderrelaties hoeven te worden gerapporteerd. De organisatorische aandacht ligt op het ontwerp en de implementatie van de maatregelen. Daarnaast is er een informatievoorziening naar het management om daar bewustwording te creëren op de risicobeheersing en de noodzaak in de organisatie te verankeren. Het implementeren van een duidelijke beveiligingsorganisatie met heldere verantwoordelijkheden en een effectief verantwoordingsproces is in deze eerste fase voorwaarde om naar een geavanceerder niveau van *performance management* te gaan.



Gedefinieerd niveau

Op het gedefinieerde niveau is het integrale securityconcept gedefinieerd en in ieder geval al voor een belangrijk deel geïmplementeerd. Doelstellingen zijn nu om de geïmplementeerde maatregelen in stand te houden. Daarbij gaat het om het aantoonbaar maken dat maatregelen bestaan en werken en dat deze goed worden beheerd. Maar ook dat de dienstverleningsrelatie van de verschillende in- en externe *security service providers* goed gedefinieerd en uitgevoerd zijn. Ten slotte moeten ook de bewustwording, kennis en kunde van betrokkenen in de risicobeheersing worden beheerd. De managementinformatievoorziening zal nu hoofdzakelijk vanuit elektronische

wegen worden gevoed. Een geïntegreerde *business intelligence tool* zal noodzakelijk zijn om deze meetgegevens in op te vangen, te analyseren en tot rapportagevormen om te werken. Op verbeterenniveau zal niet alleen het bestaande beveiligingsniveau worden beheerd, maar zullen ook zwakkere beveiligingsmaatregelen en zwakkere prestatie-indicatoren worden vervangen door effectievere. Ook zal de bewustwordingsaanpak veel meer op functie- en teamniveau worden toegevoerd.

Geïntegreerd niveau

Op geïntegreerd niveau is het integrale securityconcept volledig geïmplementeerd en zullen continu verbeteringen »

	Basis	Gedefinieerd	Geïntegreerd
Security concept	» Beperkt gedefinieerd	» Gedefinieerd » (Grotendeels) geïmplementeerd	» Concept geïmplementeerd » Continue verbetering
Doelstellingen	» Stakeholder georiënteerd » Implementatie proces	» Aanwezigheid en functioneren van gedefinieerde maatregelen » Kennis op risicobeheersing » Aansturen security service providers	» Snelheid van aanpassingsvermogen » Oorzaak & gevolg relaties » Level of effort
Informatie	» Hoofdzakelijk handmatig » Tijdelijke sheets	» Hoofdzakelijk elektronische verwerking » Beheersing intelligence tool	» Dashboard
Verbetering	» Ontwerp security concept » Ontwerp organisatie & verantwoordelijkheden » Verantwoording proces » Bewustwording op management niveau	» Externe verantwoording » Operationeel beheer van security » SLA-definitie and -mgnt » Verbeteren zwakke maatregelen » Bewustwording op team niveau	» Vergroten aanpassingsvermogen » Security gericht maken op bepaalde risico's » Verbeteren proceskosten van security » Bewustwording op individueel niveau

plaatsvinden. De doelstellingen bij dit niveau liggen op het veel sneller kunnen inspelen op dreigingen, op wisselende beveiligingsniveaus en op het nog gericht afstemmen van beveiligingsmaatregelen op bepaalde dreigingen. Daarbij wordt verder gewerkt aan het verkrijgen van een nog groter inzicht in het functioneren van de beveiliging met prestatiekenmerken die oorzaak-en-gevolgrelaties kunnen weergeven. Dit inzicht wordt ook gebruikt om de beveiligingsproceskosten in criteria als doorlooptijd, kosten en mankracht verder te optimaliseren.

De bewustwordingsaanpak zal op dit niveau meer op het individu kunnen worden afgestemd. De ondersteuning vanuit de informatievoorziening zal nog verder zijn gericht op de werkwijze van individuele managers, waarbij ook gedacht kan worden aan dashboardachtige functies.

Succesfactoren

De belangrijkste succesfactoren in het groeien in *performance* management zijn de volgende.

- » Implementeer in samenhang het hele proces. Dat bestaat in de meest elementaire vorm uit het definiëren van de succesfactoren en prestatiekenmerken, het vormen van managementinformatie uit deze prestatiekenmerken en ten slotte uit het handelen en verbeteren door alle betrokkenen die invloed hebben op de security.
- » Zorg voor balans door gebruik te maken van een volwassenheidsmodel. Zorg dat eerst alle vaardigheden op een bepaald niveau geïmplementeerd zijn, voordat vaardigheden op een hoger niveau worden gebracht.
- » Als de organisatie al over een *performance* managementaanpak beschikt, sluit daar dan op aan en verbijzon-

der de aanpak voor security. Dat is de eenvoudigste manier om aan te sluiten op de *business*-eisen van de organisatie en er kan gebruik worden gemaakt van ict-tooling en ervaringen op de managementaanpak op verbeteringen.

- » Besteed in de beginfase voldoende tijd aan het definiëren van de prestatiecriteria en bijbehorende meetgegevens. Deze prestatiecriteria vinden hun weerslag in de managementinformatie en in de organisatorische gerichtheid op het behalen van deze prestaties. Verkeerde prestatiecriteria leiden snel tot teleurstellingen in de systematiek.
- » Voer verschillende activiteiten uit om betrokken personen en partijen die invloed hebben op de security te informeren en te motiveren.

Resultaat

Het resultaat van *performance* management is een actiemodel voor management en medewerkers om de securityprestatie van de organisatie doelgericht en continu te verbeteren. Hierbij gaat het om:

- » een gestructureerde aanpak die zich richt op bereiken van securitydoelstellingen. Door het formuleren van *performance*-indicatoren worden abstract geformuleerde doelstellingen veel concreter gemaakt, waarmee het praktisch behalen van die doelstellingen ook beter in zicht komt;
- » accurate rapportages naar management en belanghebbenden over de securityprestatie. Deze transparantie helpt het management om de securityfunctie om te vormen van een ad hoc en voor velen mistig managementgebied naar een regulier managementproces;
- » een hulpmiddel om verantwoording af te leggen. Deze verantwoording kan binnen de organisatie liggen,

maar ook van en naar externe partijen zijn;

- » verantwoordingsproces op de gedefinieerde en bestaande beveiligingsmaatregelen. Op afdelingsniveau kan op basis van deze informatie direct het beheer worden verbeterd. Door deze rapportages te aggregeren wordt ook in groter verband helder of het bouwwerk van de securityfunctie nog intact is en functioneert;
- » vergroten van het inzicht in de security voor besluitvorming op verbetering van de inrichting van security, budgetten en dergelijke. De basis voor het succes ligt in het verkrijgen van inzicht in de eigen operatie, bewustwording van inefficiënties en daarmee de mogelijkheden tot prestatieverbetering. Inspraak zonder inzicht leidt tot uitspraken zonder uitzicht;
- » een aanpak die security levend houdt bij betrokken partijen. Dit kunnen klanten, medewerkers, beveiligingsorganisatie, management en andere belanghebbenden zijn. Zo kunnen rapportages over de prestatie van het eigen verantwoordelijkheidsgebied stimulerend en motiverend werken bij de direct betrokkenen;
- » en ten slotte een hulpmiddel om de gespecialiseerde securitystaf efficiënter in te zetten op die locaties en issues die de meeste support nodig hebben.

Conclusie

In twee artikelen is verkend wat *performance* management kan betekenen voor de securityfunctie. Voor complexe organisaties kan het voor de security manager een belangrijk instrument zijn om inzicht te krijgen in de securityfunctie en deze te verbeteren. Er zijn nogal wat *performance* managementmodellen en -aanpakken. De belangrijkste aspecten en succesfactoren zijn behandeld in een *performance* managementmodel dat tot de kern was teruggebracht. Vanzelfsprekend bevat het groeimodel via de verschillende volwassenheidsniveaus ook arbitraire keuzes. Van belang is dat de lijn van het betoog kan worden toegepast bij de implementatie van *performance* management in de eigen organisatie. «

*Drs. Joris Hutter RSE RCE, Hutter Security Risk Management

Samenvatting

- » Een organisatie kan systematisch en effectief groeien in haar securityprestatie. Daarin worden drie niveaus onderscheiden - basis, gedefinieerd, geïntegreerd - om te komen tot een **volwassenheidsmodel**.
- » Het **resultaat** van *performance* management is een actiemodel voor management en medewerkers om de securityprestatie van de organisatie doelgericht en continu te verbeteren.