

EEN HEK IS GEEN SECURITY

In onderstaand artikel beogen auteurs aan de hand van het 7-S model van Mckinsey dat security meer is dan allee het nemen van fysieke en/ of organisatorische maatregelen. Via de 7-S invalshoek wordt gezien wat er bij een 'goed' security- beleid allemaal komt kijken

Joop F. Verdonk
Birgitta G. van der Touw

INLEIDING

In 1980 schreven Robert Waterman, Thomas Peters en Julien Phillips "Structure is not organization"ⁱ. In dit artikel benadrukten de auteurs dat organisatie en structuur in de praktijk te vaak als synoniemen gezien werden. Waterman, Peters en Phillips betoogden daarentegen dat structuur slechts één van de factoren is die de inrichting van een organisatie bepalen.

De verwarring tussen organisatie en structuur leidde er ook toe dat oplossingen voor problemen in de organisatie te vaak gezocht werden in veranderingen binnen de structuur, zonder aandacht te besteden aan andere elementen. In veel gevallen bleek een dergelijke structurele oplossing niet of nauwelijks bij te dragen aan verbetering van de effectiviteit van de organisatie.

Volgens Waterman c.s. moeten bij het antwoord op de vraag '... how to organize better.' veel meer gegevens uit de organisatie betrokken wordenⁱⁱ. De centrale idee in de theorie is dat de effectiviteit van de organisatie bepaald wordt door de interactie van verschillende factoren. Deze elementen, allemaal met beginnend met een S, vormen tezamen het 7-S model van McKinsey.

De kritische lezer zal zich langzamerhand afvragen wat deze theoretische inleiding te maken heeft met security en criminaliteitsrisico's. Het antwoord is simpel. Het 7-S model biedt een interessante ingang om security binnen een organisatie eens nader aan een kritische beschouwing te onderwerpen.

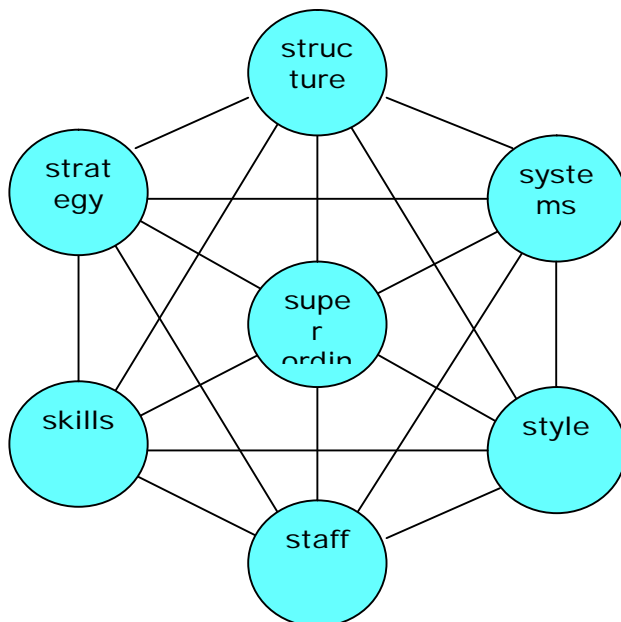
Onze stelling is dat een effectief beleid op het terrein van security en criminaliteitsbeheersing in het algemeen een samenhangend geheel vormt waarvan ieder van deze 7 factoren expliciet deel uitmaakt. Pas dan is sprake van een complete en weloverwogen aanpak van 'security-management', welke tot uitdrukking komt in een uitgebalanceerd pakket van beveiligings- en risico-reducerende maatregelen.

Hoe en waarom beveiliging benaderd wordt met de zeven S-en van McKinsey, zetten we in het vervolg uiteen. Eerst wordt het algemene 7-S model toegelicht. Daarna richten we ons op toepassing in de security.

DE 7 S-EN VAN MCKINSEY

De zeven S-en staan voor de (engelse) begrippen Structure, Strategy, Systems, Style, Staff, Skills en Superordinate goals. In het model is elk element verbonden met de anderen (zie figuur 1). Voor een manager biedt elke factor een potentieel aangrijpingspunt

om de organisatie in de gewenste richting te sturen. Omdat alles echter met alles samenhangt heeft een verandering in één van de factoren automatisch effect op de anderen. De invoering van een nieuw systeem bijvoorbeeld, lijdt onherroepelijk tot structuurwijzigingen.



$7 \times S + \text{Security} = 8S$

Figuur 1. Het 7-S model van McKinsey

Ontleend aan: Waterman, R.H.jr., Th.J. Peters, J.R. Phillips,

Structure is not organization, in: Business Horizons June 1980

De S-en laten zich als volgt beschrijven.

Structure is de wijze waarop de organisatie is opgebouwd, de onderlinge taakverdeling, de inhoud van de taken en de samenhang/ coördinatie ervan

Strategy behelst de activiteiten die een organisatie denkt te ondernemen, anticiperend op veranderingen in haar omgeving. Met de gekozen strategie verwacht de organisatie haar doelen te bereiken, haar positie te verbeteren om zich gunstig van anderen te onderscheiden. Met de *strategy* stelt de organisatie prioriteiten in de aanwending van haar middelen.

Systems zijn alle formele en informele procedures, regelingen en afspraken die in de organisatie toegepast worden. Kennis van de systemen binnen de organisatie is een voorwaarde voor beheersing en beïnvloeding van de organisatie.

Style heeft betrekking op de cultuur van de organisatie. Tot de stijl behoren de manier van handelen, de wijze van aanpak en uitvoering die de organisatie kenmerken. De stijl uit zich in het gedrag van het management en de medewerkers.

Staff verwijst naar de medewerkers van de organisatie in de brede zin van het woord. Het begrip omvat de meest uiteenlopende aspecten, die betrekking hebben op personeel: van beoordelingssystemen, salarisschalen etc. tot moraal, motivatie e.d.

Skills zijn de opvallende bijdragen, vaardigheden en bekwaamheden van de (medewerkers in) de organisatie waardoor zij zich profileert ten opzichte van andere organisaties.

Superordinate goals zijn de 'bovenliggende' doelstellingen binnen de organisatie die door iedereen gedeeld worden.

Waterman c.s. doelen met deze aanduiding op (vaak ongeschreven) waarden en aspiraties, die leidend zijn voor de activiteiten binnen de organisatie. Superordinate goals gaan verder dan de geformuleerde doelstellingen van de onderneming. Het vormen bindende krachten in een organisatie, die door iedereen onderschreven worden. De superordinate goals vormen de kern van de corporate identity.

DE ZEVEN S-EN EN SECURITY-MANAGEMENT

Zoals 'structuur' geen synoniem is voor 'organisatie', zo is 'beveiliging' niet hetzelfde als 'security-management'. Het 7-S model onderschrijft de stelling dat een prachtige organisatiestructuur nooit een garantie is voor een effectieve organisatie. Aan de hand van dit Mc Kinsey-model van McKinsey zullen we aantonen dat security veel verder gaat dan fysieke beveiliging van een organisatie, door middel van hekwerken, infraroodinstallaties of manbewaking. Wij gebruiken de begrippen 'security' en 'security-management' door elkaar, in de brede betekenis van deze woorden.

Structure en security

Het woord 'structuur' heeft in criminaliteitsmanagement twee betekenissen.

In de eerste plaats is dat organisatiestructuur. Security zit in de organisatie altijd in een bepaalde structuur gegoten. In navolging van Waterman c.s. verstaan we onder structuur hier de opbouw van de organisatie, de taak- en bevoegdhedenverdeling, de taakinhoud, etc.

Deze structuur bepaalt vaak in hoge mate de effectiviteit van de beveiliging. Toch wijst de praktijk uit dat de coördinatie in veel organisaties ver te zoeken is: sleutelbeheer is een (vergeten) taak van de portier, aangifte plicht ontbreekt, en het externe beveiligingsbedrijf is ingehuurd door een medewerker van financiën, die zich bewust is van *een* probleem. Hij weet echter niet precies welk probleem.

Welke invulling van de functies en verantwoordelijkheden op het gebied van beveiliging

effectief is, hangt onder meer af van de aard van de organisatie. In een hele klein bedrijf is security sterk afhankelijk van de top van de organisatie, vaak de ondernemer persoonlijk. Binnen een gedivisionaliseerde organisatie liggen verantwoordelijkheden veel lager omdat iedere divisie zijn eigen lokale problemen heeft, waarvan de divisie-directeur het meest afweet. Beveiliging in een professionele organisatie, zoals bijvoorbeeld een ziekenhuis, is afhankelijk van de kwaliteit van de staffunctionarissen, die dit in hun portefeuille hebben. De professionals zien criminaliteit vrijwel nooit als een probleem dat zij zelf moeten aanpakken: "Daar is het management voor."

Naast een organisatiestructuur kent iedere organisatie ook een fysieke infrastructuur. Deze is in de eerste plaats belangrijk bij de inventarisatie van de risico's die een bedrijf loopt. Hierbij spelen factoren zoals de plaats van vestiging, toevoerwegen, nabijheid van buurbedrijven en ook de infrastructuur in de zin van gebouwen, bouwmaterialen e.d. een grote rol.

Bij het ontwerpen van maatregelen zijn deze elementen opnieuw van belang. Het klinkt enigszins paradoxaal, maar de infrastructuur stelt enerzijds bepaalde eisen aan de mate van beveiliging, maar anderzijds ook grenzen aan de mogelijkheden van beveiliging.

Strategy en security

De keuze die de organisatie maakt in het gebruik van haar middelen bepaalt de strategie, en daarmee de richting van de organisatie in de toekomst. Idealiter wordt risico-management in het algemeen, dus ook security-management, geïntegreerd betrokken bij zowel de ontwikkeling van strategie als de dagelijkse bedrijfsvoering van een onderneming. In de praktijk valt dit tegen. Aandacht voor ondernemersrisico's is geaccepteerd; criminele risico's lijken echter ver weg.

Strategie is belangrijk zowel bij risico-inventarisatie als in de sfeer van maatregelen. De strategische beslissingen over producten en markten verwijzen direct naar kwetsbare punten in de organisatie.

Ook in de uitwerking van deze strategie worden criminele dreigingen gesignaleerd. Het middenkader houdt zich op tactisch niveau bezig met middelen die nodig zijn, en de randvoorwaarden om de strategische beslissing in te vullen. Op de werkvloer tenslotte komen directe signalen over risico's uit de operationele contacten met klanten.

In de beleidsontwikkeling ten aanzien van security keert deze driedeling strategisch, tactisch en operationeel terug.

Het topmanagement stuurt op hoofdlijnen, coördineert en stelt kaders. De functionele invulling is een tactische taak van het middenkader en op de werkvloer vindt de feitelijke uitvoering plaats, waarbij de praktijk een toetssteen vormt.

Systems en security

In iedere organisatie worden allerlei systemen opgetuigd om de organisatie te sturen. Tot systemen rekenen we alle formele en informele procedures, die een organisatie draaiende houden. Voorbeelden zijn budgetteringssystemen, informatiesystemen, productie- en logistieke systemen.

Tegelijkertijd genereren deze systemen echter ook risico's in de organisatie. Een

beschadigd systeem vormt een probleem voor de organisatie. Bij iedere risico-inventarisatie moet daarom systematisch aandacht aan de kwetsbare systemen geschonken worden.

Hoe structuur en systeem risico's oproepen blijkt uit het voorbeeld van de financiële administratie van een bedrijf. Financiële procedures en de bijbehorende verdeling van bevoegdheden zijn vaak historisch gegroeid. Een kritische bezinning hierop toont soms dat de scheiding van bevoegdheden bij aangaan, afhandeling en controle van transacties vaak te wensen overlaat, waardoor potentiële fraudebronnen ontstaan.

Opnieuw paradoxaal is dat de organisatie er niet aan ontkomt om de bestaande systemen te beveiligen met invoering van nieuwe systemen: Nieuwe informatielijnen, andere procedures, maar ook wellicht elektronische beveiligingssystemen.

Style en security

Een cruciale factor bij de invoering van nieuw beleid vormt de cultuur. Geen enkele manager kan kennis van de heersende normen en waarden missen bij zijn besluitvorming. Cultuur bepaalt de haalbaarheid van maatregelen, en legt noodzakelijke organisatie-ontwikkelingen en gedragsveranderingen van medewerkers bloot.

De rol van het (top)management bij deze ontwikkelingen is een bepalende. Afleren van ongewenst gedrag van medewerkers is uitermate lastig, hoe zinvol maatregelen objectief beschouwd ook zijn. Als het gedrag van de manager dan niet als voorbeeld geldt, is het effect helemaal nihil. En dit voorbeeldgedrag moet zich niet alleen uiten in woorden, maar veel meer in daden. Een procedure betreffende 'clean-desk' buiten werktijd sorteert geen effect als de topmanager deze regels zelf regelmatig met voeten treedt.

Omdat cultuurverandering zo gecompliceerd is, bieden oplossingen het meest perspectief als de ondernemer zoveel mogelijk aansluit bij het bestaande gedrag. Het is echter niet uitgesloten dat in bepaalde situaties een cultuurverandering noodzakelijk blijkt, met alle consequenties voor de rest van de organisatie van dien.

Skills en security

Voordat de organisatie daadwerkelijk overgaat tot de invoering van security-maatregelen is het noodzakelijk dat het management zich rekenschap geeft van het belang van security voor de bedrijfsvoering. Soms is security namelijk van ondergeschikt belang; slechts af en toe blijkt het een element te zijn dat de kwaliteit van het eindproduct bepaalt.

Voor een luchthaven bijvoorbeeld kan het veiligheidsniveau de bepalende factor zijn in de concurrentie strijd. Dat betekent dat de maatregelen op een heel ander niveau zullen liggen en van totaal andere aard zullen zijn dan de beveiliging van een wolfabriek tegen criminele dreigingen.

Skills zijn de elementen waarmee de organisatie zich onderscheidt. Zij bepalen het imago van de onderneming naar de klant. Soms blijkt de gekozen strategie het noodzakelijk te maken dat de organisatie nieuwe skills leert. Security bewustzijn is voor luchthavens vooral belangrijk geworden na de terroristische aanslagen in de jaren '70.

Staff en security

Medewerkers vormen de sleutel tot succes. Hun gedrag bepaalt de effectiviteit van security. Zorgvuldig omgaan met security komt daarom tot uiting in zorgvuldig gekozen personeelsbeleid.

De inhoud van dit personeelsbeleid is afhankelijk van de organisatie. Soms is een centrale rol weggelegd voor training en opleiding, niet alleen in vaardigheden (bijvoorbeeld bij de confrontatie met een bankoverval, het onthouden van signaleringen etc.), maar ook met het bewuste doel gedrag te veranderen en het risico bewustzijn te verhogen.

Personeelsbeleid stopt niet bij opleiding. Security management behoort ook aandacht te hebben voor opvang van slachtoffers.

Daarnaast is beloning bijvoorbeeld een mogelijk aangrijpingspunt. Het uitloven van een prijs voor het beste idee op het terrein van security vergroot de betrokkenheid van medewerkers.

Een zorgvuldig personeelsbeleid uit het oogpunt van security begint reeds bij de aanname van nieuw personeel. Goede selectie en een antecedentenonderzoek voorkomen veel problemen.

Superordinate goals en security

Superordinate goals zijn een soort 'meta-doelstellingen'. Het zijn fundamentele ideeën, waarop de onderneming gebouwd is. In het artikel geven Waterman c.s. als voorbeelden 3M (nieuwe producten) Hewlett Packard (innovatieve mensen op alle niveau's) en IBM (service)ⁱⁱⁱ.

Superordinate goals reikt dus verder dan cultuur en sleutelvaardigheden. Deze twee passen zich aan, wanneer de koers van de organisatie verandert. Superordinate goals daarentegen liggen ten grondslag aan de strategische richting van de organisatie.

Opvallend is dat in alle succesvolle organisaties in veel gevallen superordinate goals aangetroffen worden.

In security kan dit concept in het verlengde liggen van wat we opgemerkt hebben onder skills. Beveiliging, veiligheid, een veilig gevoel zowel van klanten als medewerkers kan tot een waarde worden, die organisatie-breed gedragen wordt. In dat geval is iedere medewerker doortrokken van het besef dat ieder product van het bedrijf, wat het dan ook is, in ieder geval de toets van security moet doorstaan.

8 S-EN: EEN BRUIKBAAR CONCEPT

In het voorafgaande hebben we een relatie gelegd tussen Security en de 7 S-en van Mc Kinsey. Onze stelling is dat een security-audit aan de hand van dit model enerzijds een compleet beeld geeft van de bestaande situatie op security-gebied binnen de organisatie, en anderzijds een ingang kan bieden om toekomstig beleid te ontwikkelen.

In ieder geval zijn vier functies te onderscheiden, die voor een deel in elkaars verlengde liggen:

1. monitoring van de bestaande situatie
2. definiering van de gewenste situatie, waarbij een risico-inventarisatie belangrijk onderdeel vormt
3. inventarisatie van knelpunten
4. formulering van beleid en opstellen van een beveiligingsplan.

Het behoeft geen toelichting dat deze cyclus een iteratief proces is, omdat ieder beleid na enige tijd evaluatie behoeft.

Het model toont tevens aan dat security(-management) veel meer omvat dan vaak aangenomen wordt. Beveiliging houdt niet op bij het plaatsen van een hekwerk. Integendeel, de hele organisatie is er bij betrokken. Gedrag, waarden en normen spelen een centrale rol.

Oegstgeest 2005

Joop F. Verdonk, Manager Corporate Security N.V.Luchthaven Schiphol

Birgitta G. van der Touw, Adviseur Management Development Technische Universiteit te Delft, o.m. werkzaam bij Mertens en Partners B.V., Consultants voor Politiemanagement en Criminaliteitsbeheersing.

- i.. Waterman, R.H.jr., Th.J. Peters, J.R. Phillips, **Structure is not organization**, in: Business Horizons June 1980.
- ii.. Zie ook **The Art of Japanese Management**, by R.T. Pascale and A.G. Athos, Warner Books Inc., New York, 1981.
- iii.. Waterman, R.H.jr., Th.J. Peters, J.R. Phillips, **Structure is not organization**, in: Business Horizons June 1980, p. 25.