

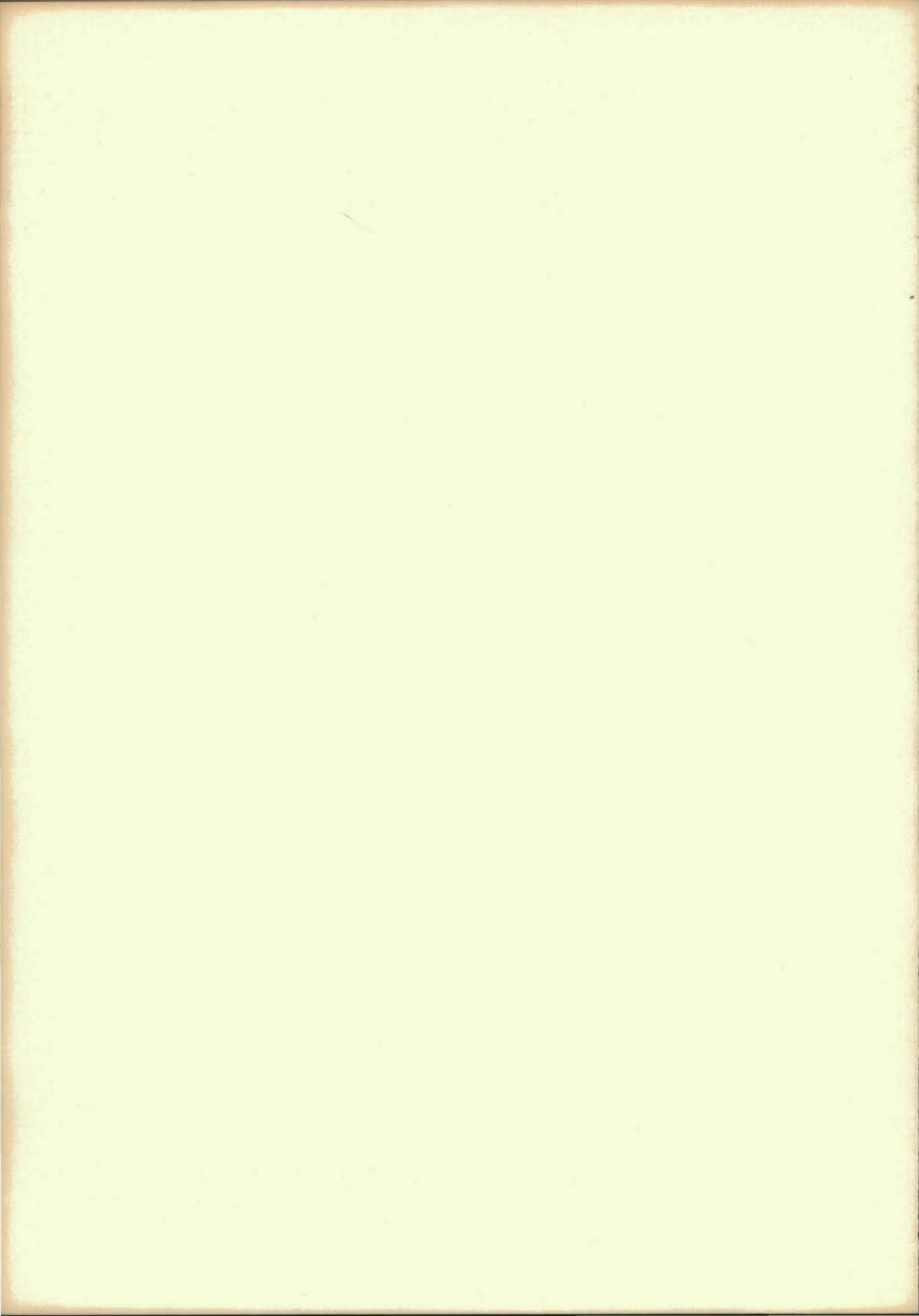
Landelijk Bureau Voorkoming Misdrijven

Beveiliging bedrijfsvestigingen



Voorkoming misdrijven
'n Zaak van de politie én u

92/50





Landelijk Bureau Voorkoming Misdrijven

Beveiliging bedrijfsvestigingen

Woord vooraf

In deze brochure worden methodieken beschreven die u op weg kunnen helpen bij de beveiliging van uw bedrijf. Deze methodieken zijn in de afgelopen jaren ontwikkeld door Voorkoming Misdrijven.

De organisatie Voorkoming Misdrijven kent, bij de verschijning van deze brochure, op het landelijk niveau het Landelijk Bureau Voorkoming Misdrijven (LBVM). Het LBVM is ondergebracht bij de Directie Criminaliteitspreventie van het ministerie van Justitie. Eerstverantwoordelijke voor de criminaliteitspreventie is de staatssecretaris van Justitie, de minister van Binnenlandse Zaken draagt mede verantwoordelijkheid. Regionaal zijn er 23 bureaus Voorkoming Misdrijven (RBVM) bij de politie, terwijl ook de koninklijke Marechaussee en de Rijkspolitie te water participeren.

Als gevolg van de reorganisatie van de Nederlandse politie staat de VM-organisatie als een aparte organisatorische voorziening binnen de regio's ter discussie. Met de regionalisering van de politie wordt de politieke preventie opnieuw vormgegeven. De Voorkoming Misdrijven-structuur zal op regionaal en lokaal niveau met de invoering van de regionale politiekorpsen verdwijnen. Het Landelijk Bureau Voorkoming Misdrijven wordt eerder, namelijk per 1 januari 1993 opgeheven.

Op het moment van verschijning van deze brochure is het nog niet geheel duidelijk op welke wijze de criminaliteitspreventie binnen de regionale politie organisatorisch wordt ingevuld. Bovendien zal de functionele inbedding per regio verschillen. Hierdoor is het niet mogelijk om in deze brochure aan te geven bij wie u, na de reorganisatie van de politie, aan het juiste adres bent voor aanvullende tips en adviezen.

Gedurende de reorganisatie kunt u voor advies en hulp nog contact opnemen met het Bureau Voorkoming Misdrijven in uw regio. Na de reorganisatie kunt u informeren bij uw politie wie voor u de aangewezen adviseur is.

Inhoudsopgave

	Pagina:
1 Inleiding	5
2 De filosofie	6
2.1 Beveiliging is meer dan sloten, toeters en bellen	6
2.2 Beveiligen op vier niveaus	6
2.3 Top down/bottom up	8
2.4 Beveiliging is teamwork geworden	9
3 De aanpak	10
3.1 De kleurenmethode	10
3.2 De wielenmethode	14
3.3 De twee methoden samengevoegd tot een plan van aanpak	16
Literatuur	19
Adressen	19
Colofon	20

1 Inleiding

Het bedrijfsleven wordt bijzonder vaak slachtoffer van criminaliteit. Zo was in 1988 maar liefst 55% van het totaal aantal misdrijven in Nederland gericht tegen het bedrijfsleven. Als we de uitkomsten van een aantal onderzoeken naar criminaliteit tegen het bedrijfsleven combineren, kunnen we de volgende tabel samenstellen.

Tabel 1: Enkele vormen van criminaliteit tegen bedrijven

delicten	percentage slachtoffers %	aantal delicten per jaar abs.	totale schade per jaar (x 1 miljoen gld)
criminaliteit door derden (extern):			
vernietiging	23	474.000	363
inbraak	21	214.000	632
diefstal	13	300.000	511
bedreiging en beroving	8	198.000	40
brandstichting	(< 0,5%)	400	96
winkeldiefstal	63	2.545.000	1.359
verzekeringsfraude	?	?	400
criminaliteit door eigen werknemers (intern):			
	11	303.000	447
totaal	?	4.035.000	3.848

Bronnen: gegevens NVB (bankovervallen); van Hoek, 1989 (brandstichting); Centraal Informatiesysteem Schade (verzekeringsfraude); Criminaliteit en detailhandel, 1991 (winkeldiefstal); Bedrijfsleven en criminaliteit, 1990 (overige delicten).

Uit de tabel blijkt dat het bedrijfsleven jaarlijks getroffen wordt door ruim 4 miljoen gevallen van criminaliteit. Dit levert een totale jaarlijkse schade op van ruim 3,8 miljard gulden (in 1 jaar tijd). Vooral diefstallen en inbraken veroorzaken veel schade, en er is dan ook alle reden voor bedrijven om zich goed te beveiligen tegen deze risico's.

In deze brochure wordt een methode beschreven, waarmee u stap voor stap de beveiliging van een bedrijfsvestiging kunt aanpakken. De brochure is bedoeld om eigenaars en beheerders van bedrijfsgebouwen inzicht te geven in de problemen rond de beveiliging van hun gebouwen. De brochure is met name gericht op de beveiliging van middelgrote bedrijven. Voor de zeer kleine bedrijven zal beveiliging vaak een wat eenvoudiger aangelegenheid zijn, terwijl aan de complexe problematiek van grote bedrijven weinig recht kan worden gedaan in deze brochure.

2 De filosofie

2.1 Beveiliging is meer dan sloten, toeters en bellen

Er zijn nog steeds mensen die denken dat beveiliging van bedrijfsgebouwen niet meer is dan het aanbrengen van voldoende sloten, grendels, tralies, detectoren of alarminstallaties. Deze mensen zien over het hoofd dat een te beveiligen bedrijfsgebouw een medaille is die twee kanten heeft:

- het gebouw zelf: de 'harde' fysieke structuur (muren, deuren, ramen, daken, etc.) en
- de menselijke organisatie die **in** dat gebouw werkzaam is: de mensen, de goederenstroom, de activiteiten, kortom het bedrijfsproces en de bedrijfscultuur.

Een gebouw zonder inhoud is niks (een dood ding) en een inhoud zonder gebouw is ook niks, zeker in ons gure Nederlandse klimaat. Toch ziet men bij beveiliging deze simpele waarheid maar al te vaak over het hoofd. Men gaat dan het gebouw fysiek beveiligen en vergeet dat beveiligingsmiddelen door de mensen c.q. de organisatie **in** het gebouw, gebruikt moeten worden. Als de fysieke beveiliging niet naadloos past in het bedrijfsproces en de bedrijfscultuur, is de beveiliging niet effectief.

Men vergeet bij beveiliging ook vaak dat de beveiligingsmiddelen niet in de eerste plaats bedoeld zijn om het gebouw te beveiligen, maar dat het uiteindelijke doel vooral is dat het bedrijfsproces ongehinderd kan blijven doorgaan. Beveiliging die de medewerkers stoort in de uitvoering van hun taken, zal nooit werken.

Als men het bedrijfs**proces** (en niet het bedrijfsgebouw) tot uitgangspunt neemt, en rekening houdt met de mensen die in het bedrijf werken, komt men vaak tot andere en betere oplossingen van beveiligingsproblemen: naast technische maatregelen kunnen ook veranderingen in het bedrijfsproces en de bedrijfscultuur bijdragen aan een beter beveiligde organisatie.

2.2 Beveiligen op vier niveaus

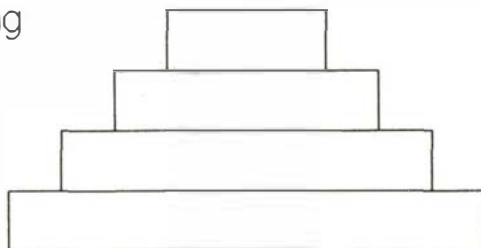
In figuur 1 wordt onderscheid gemaakt tussen vier niveaus die bij beveiliging van belang zijn. Op de onderste tree ligt het accent op de beveiligingsmiddelen: de elektronische en bouwkundige beveiligingsprodukten. Op de bovenste tree ligt het accent op het karakter van de te beveiligen organisatie: de doelen, strategieën, structuur en cultuur van de organisatie, verder kortweg aangeduid als de 'bedrijfsvoering'.

niveau 4: bedrijfsvoering

niveau 3: gebruik

niveau 2: installatie

niveau 1: middelen



Figuur 1: vier niveaus van beveiliging

niveau 1: de beveiligingsmiddelen

Dit is de onderste tree van de (ongemonteerde) beveiligingsprodukten, die op zichzelf nog geen functie in het gebouw hebben; bouwkundige produkten als hang- en sluitwerk, gevelelementen, en elektronische produkten als sensoren, melders, alarmeren en dergelijke. Beveiligingsprodukten verschillen in kwaliteit. Een belangrijke kwaliteitsnorm zijn de normen voor inbraakwerend hang- en sluitwerk; de NEN 5088 en NEN 5089¹. Hang- en sluitwerk dat voldoet aan deze NEN-normen geven de koper dus enige zekerheid over de kwaliteit van de produkten. Maar toepassing van kwalitatief goede beveiligingsmiddelen leidt niet als vanzelf tot goede beveiliging. Met een vier-sterren racemotor is men op het circuit nog geen winnaar. Die motor moet immers wel goed geïnstalleerd worden in een vier-sterren chassis en daarnaast moet dan ook nog sprake zijn van een goede coureur en een perfecte organisatie.

Overigens zij opgemerkt dat middelen niet per sé technische middelen hoeven te zijn. De Romeinen gebruikten al ganzen als luid alarm en tegenwoordig vervullen honden soms deze rol. Daarnaast zijn natuurlijk ook mensen in veel situaties goede 'beveiligingsmiddelen', met als bijkomend voordeel dat ze allerlei neventaken kunnen vervullen (portier, receptionist).

niveau 2: plaats, montage en installatie van middelen

De preventieve werking van de middelen is afhankelijk van een juiste plaatsing, inbouw en installatie. De juiste onderlinge samenhang van de toegepaste middelen is daarbij essentieel: elke ketting is even sterk als de zwakste schakel.

Zo komt het bij beveiliging tegen inbraak wel eens voor dat de deuren zeer goed beveiligd zijn, terwijl de ramen - en dat hoeft er maar één te zijn - vergeten worden; of men monteert een prima slot op goede wijze in een stevige deur, maar vergeet dat elk slot een even goede en passende sluitkom nodig heeft.

Dit tweede niveau wordt samenvattend aangeduid met installatie.

niveau 3: gebruik van beveiligingssystemen

Nog een stap hoger belandt men bij de organisatie die met de geïnstalleerde middelen moet omgaan.

Beveiligingsmiddelen moeten door mensen in het bedrijfsproces eenvoudig gebruikt kunnen worden. Beveiligingsmiddelen die niet logisch passen in het bedrijfsproces blijken alras nutteloos: de kluis die elke 10 minuten geopend moet worden omdat er zaken in liggen die steeds weer nodig zijn, zal open blijven staan; de zwaar beveiligde deur die de snelle doorgang naar de koffie-automaat verhindert, treft eenzelfde lot.

niveau 4: bedrijfsvoering

Op dit hoogste niveau krijgen we te maken met de doelen van de organisatie, de structuur, de produktiewijzen en de bedrijfscultuur. Voor een goed beveiligingsbeleid is de analyse van dit niveau zeer belangrijk. Beveiligingsdoelen en -strategieën moeten goed afgestemd zijn op de bedrijfsvoering. Beveiligingsmaatregelen mogen de realisering van de hoofddoelen van de organisatie nooit belemmeren. Andersom kan het gebeuren dat de bedrijfsvoering op bepaalde punten wordt aangepast aan beveiligingsdoelen.

Beveiliging op dit niveau begint met een bewustwording van de risico's. Deze bewustwording zal van boven naar beneden als een rode draad door de gehele organisatie moeten lopen. De heersende cultuur, de formele en informele communicatie en de verdeling van verantwoordelijkheden spelen hierbij een belangrijke rol.

¹ NEN 5088: Inbraakveiligheid van gebouwen - Bouwtechnische beveiliging van woningen - Toepassing van hang- en sluitwerk. NEN 5089: eisen en beproevingsmethoden. Verkrijgbaarheid: zie adressenlijst achterin.

Belangrijke maatregelen op het niveau van de bedrijfsvoering zijn:

- * Het optimaliseren van bedrijfsprocessen in het licht van criminaliteitspreventie. Dat wil zeggen het verlagen van de kwetsbaarheid van de organisatie voor criminaliteit, door bijvoorbeeld procedures te wijzigen, routes van kwetsbare goederen te verleggen of bepaalde activiteiten te verplaatsen naar een gunstiger tijdstip.
- * Veranderingen in de bedrijfscultuur: het verhogen van het risico-bewustzijn van de medewerkers en het verbeteren van de houding ten aanzien van criminaliteitspreventie door communicatie, voorlichting, opleiding en het opnemen van preventief werken in de reguliere beoordelingscriteria.

2.3 Top down/bottom up

Voor een goed beveiligde organisatie in een goed beveiligd gebouw is het noodzakelijk dat aan alle niveaus voldoende aandacht wordt besteed en dat er een goede wisselwerking en afstemming is tussen de vier niveaus. Bij de vormgeving en invoering van het beveiligingsbeleid ontstaan op elk niveau knelpunten die oplossingen op dat niveau vereisen, maar deze oplossingen moeten ook passen in het beleid op de overige niveaus.

In een goed beveiligingsbeleid zal dan ook, naast de veel toegepaste bottom-up (fysieke en technische) benadering, tevens de top-down (bedrijfsvoerings)benadering gehanteerd moeten worden. Daarbij zal regelmatig afstemming tussen deze trajecten plaats moeten vinden.

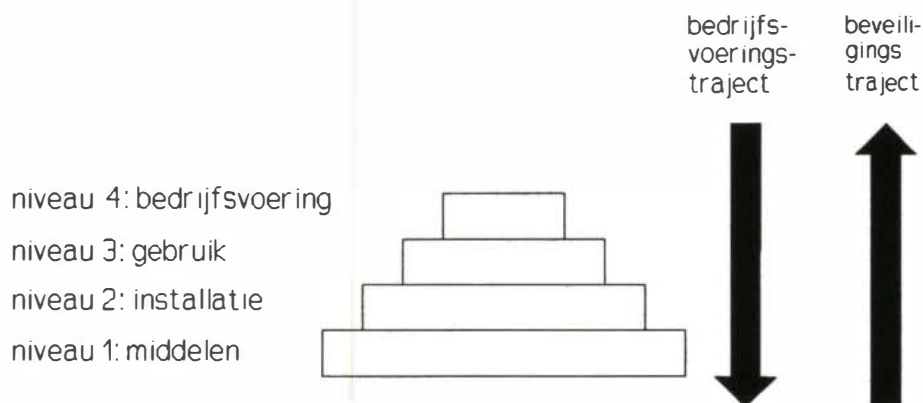
* Top-down

Dit zijn maatregelen die op het niveau van de bedrijfsvoering ingevoerd worden en die vooral gericht zijn op het optimaliseren van bedrijfsprocessen en het verhogen van het preventiebewustzijn. De kwetsbaarheid van de organisatie wordt daarmee verlaagd, wat een positieve invloed heeft op de fysieke beveiligingsbehoefte. Zo wordt de noodzaak tot het nemen van ingrijpende technische maatregelen vermindert.

* Bottom-up

Van onderop borrelen de technopreventieve of fysieke maatregelen omhoog. Het invoeren van technische maatregelen op installatieniveau heeft gevolgen voor de bovenliggende lagen: voor het gebruik van de beveiliging en voor het functioneren van de organisatie als geheel.

De aanpak die in de volgende paragraaf besproken wordt, is gebaseerd op deze filosofie en kent dus ook deze twee parallel lopende trajecten.



Figuur 2: Niveaus en trajecten

2.4 Beveiliging is teamwork geworden

Uit het bovenstaande mag duidelijk zijn, dat beveiliging niet ophoudt bij sloten, grendels, toeters en bellen. Natuurlijk blijft kennis over beveiligingsprodukten en hun installatie belangrijk. Maar naast die kennis blijkt dat een goede bedrijfsbeveiliging ook gebruik moet maken van een degelijke analyse van criminele risico's, kennis over logistiek management en een flinke portie organisatiedeskundigheid.

Bovendien zijn het succes van het beveiligingsplan en de daaruit voortkomende maatregelen in de eerste plaats afhankelijk van de betrokkenheid en commitment van de medewerkers van het bedrijf.

Daarmee is beveiliging dus een proces geworden dat bestaat uit teamwork van verschillende disciplines. Goede communicatie binnen dit team, maar ook tussen het team en de medewerkers van het bedrijf, is daarbij de sleutel tot succes.

3 De aanpak

Voorkoming Misdrijven heeft een methodiek ontwikkeld voor het beveiligen van overheids- en bedrijfsgebouwen. Hierbij wordt gebruik gemaakt van twee methoden:

- De **kleurenmethode**: een manier om criminele risico's en knelpunten in de fysieke beveiliging aanschouwelijk en bespreekbaar te maken; bovendien kunnen de (voor) genomen beveiligingsmaatregelen geëvalueerd worden met deze methode.
- De **wielenmethode**: een manier om systematisch alle 4 niveaus van beveiliging na te lopen, waarbij steeds aandacht is voor de relatie van beveiliging met de bedrijfsvoering.

Als de twee methoden in combinatie met elkaar worden toegepast kunnen de uitkomsten worden gebruikt voor het opstellen van een concreet **plan van aanpak**.

Het belangrijkste uitgangspunt van het plan van aanpak is, dat het beveiligingstraject (het bottom-up traject) en het bedrijfsvoeringstraject (het top-down traject) steeds naast en in samenhang met elkaar bekeken worden. Dit uitgangspunt komt terug in de 2 methoden.

3.1 De kleurenmethode

De kleurenmethode is een techniek waarmee op basis van plattegronden en kleuren knelpunten in de beveiliging kunnen worden aangegeven. De kleurenmethode wordt gebruikt als hulpmiddel om de risico's in beeld te brengen, om na te gaan of de bestaande beveiliging afdoende is en om, in een later stadium, de genomen of geplande maatregelen te evalueren. De kleurenmethode is vooral geschikt om zicht te krijgen op concrete criminele risico's als diefstal of vernieling van waardevolle goederen in het bedrijfsgebouw. De aan de hand van de kleurenmethode gevonden oplossingen zitten dan ook vooral op de lagere beveiligingsniveaus 1 en 2 (keuze en installatie van middelen), en hooguit op niveau 3 (gebruik van beveiligingsmiddelen).

Meer abstracte begrippen uit het bedrijfsvoeringstraject (niveau 4), zoals de bedrijfsdoelen, bedrijfsbeleid, bedrijfscultuur en risicobewustzijn, kunnen niet via de kleurenmethode aangegeven worden.

Werkwijze kleurenmethode

Bij de toepassing van de kleurenmethode wordt het bedrijfsgebouw twee keer in kaart gebracht: één keer vanuit het perspectief van de bedrijfsprocessen en één keer vanuit het perspectief van beveiliging.

Zowel in het bedrijfsvoeringstraject als het beveiligingstraject worden plattegronden van het bedrijfsgebouw gebruikt (liefst op doorzichtig materiaal), waarop met behulp van 4 kleuren wordt aangegeven waar zich kwetsbare bedrijfsgoederen en -processen bevinden (bedrijfsprocessen-plattegrond) en wat de bestaande beveiligingssituatie in het bedrijf is (beveiligings-plattegrond). Vervolgens wordt een risico-analyse gemaakt door beide plattegronden over elkaar heen te leggen. Kleurverschillen duiden dan op een onevenwichtigheid tussen beveiliging en risico.

De bedrijfsprocessen-plattegrond: kwetsbaarheid

De bedrijfsprocessen-plattegrond geeft inzicht in de plaats en routing van de belangrijkste procesgoederen (spullen, informatie, geld, etc.) en procesmiddelen (produktiemiddelen als machines, gereedschap, computers) binnen het gebouw. Daarbij wordt met kleuren aangegeven hoe kwetsbaar deze goederen/middelen zijn.

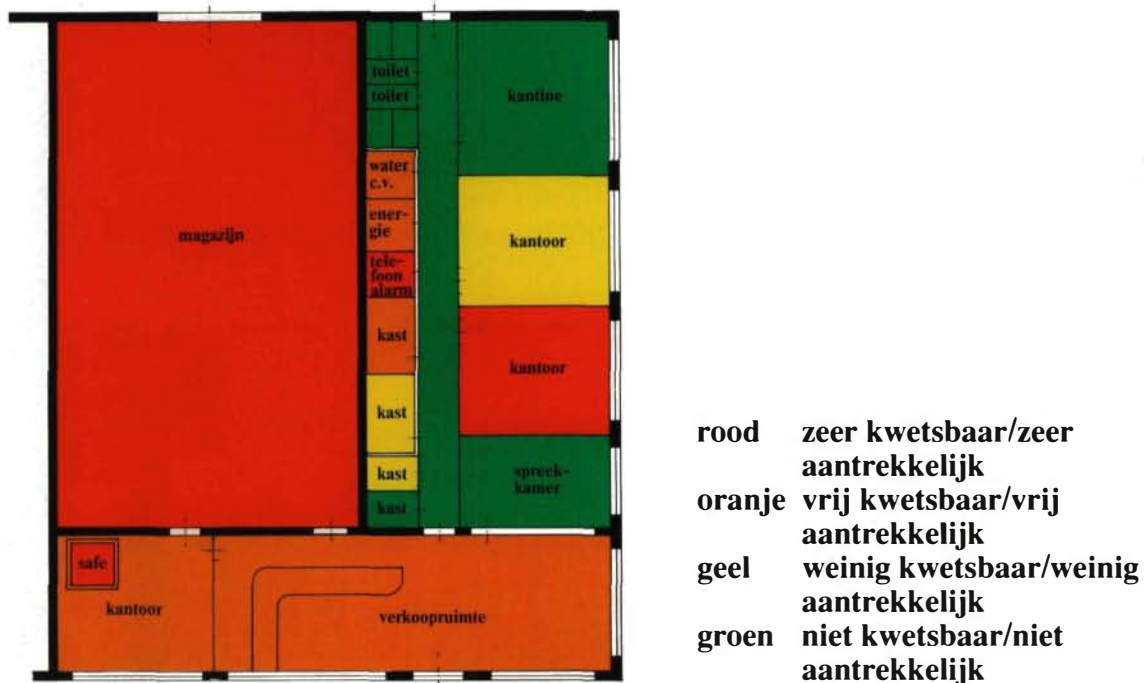
Er wordt nog geen rekening gehouden met de aanwezige beveiliging, dat komt aan de orde in de beveiligingsplattegrond.

De relatieve kwetsbaarheid van goederen en middelen wordt gemeten via:

- de waarde voor de organisatie: de gevolgen die voor de organisatie ontstaan als een goed of middel verdwijnt of in het ongereede raakt (afbreukrisico);
- de 'criminele waarde': de aantrekkelijkheid van de goederen en middelen voor een potentiële crimineel.

Beide criteria moeten in de beschouwing betrokken worden. Het hoeft niet zo te zijn dat datgene dat waarde heeft voor de organisatie ook van belang is voor criminelen en omgekeerd.

Met kleur wordt op de volgende wijze onderscheid gemaakt in de relatieve mate van kwetsbaarheid/aantrekkelijkheid:



Figuur 3: bedrijfsprocessen-plattegrond

In de figuur 3 is de bedrijfsprocessen-plattegrond afgebeeld van een groothandel in meetinstrumenten. Een gedeelte van de instrumenten is zeer kostbaar en de 'criminele waarde' van deze instrumenten is ook hoog. Het magazijn is meestal goed gevuld met meetinstrumenten en is daarom rood ingekleurd. In de verkoopruimte staan verschillende showmodellen opgesteld. Omdat het hier om een beperkt aantal gaat is deze ruimte oranje ingekleurd. In het oranje ingekleurde kantoor staan verschillende defecte en gerepareerde instrumenten. In de safe zit het kasgeld en orderboeken. In het rood ingekleurde kantoor staat de minicomputer en liggen de back-ups. De minicomputer is het hart van de administratieve bedrijfsvoering: het bedrijfsproces zou ernstig verstoord worden als er iets met deze computer gebeurt. In de oranje ingekleurde kast zit het archief van de groothandel.

Het bepalen van de kwetsbaarheid van bedrijfsgoederen en bedrijfsprocessen gebeurt bij voorkeur mede aan de hand van concrete gegevens over de criminaliteit die feitelijk plaatsvindt in/rond het bedrijfsgebouw. Dit vereist wel dat er binnen het bedrijf een goede registratie bestaat van (semi-) criminele incidenten, inclusief gegevens over mogelijke daders, plaats, tijdstip, toedracht en dergelijke. De praktijk leert dat slechts een handje vol bedrijven beschikt over een dergelijke registratie.

Het opzetten van een goede criminaliteitsregistratie kan uiteraard onderdeel uitmaken van de verbeteringsmaatregelen.

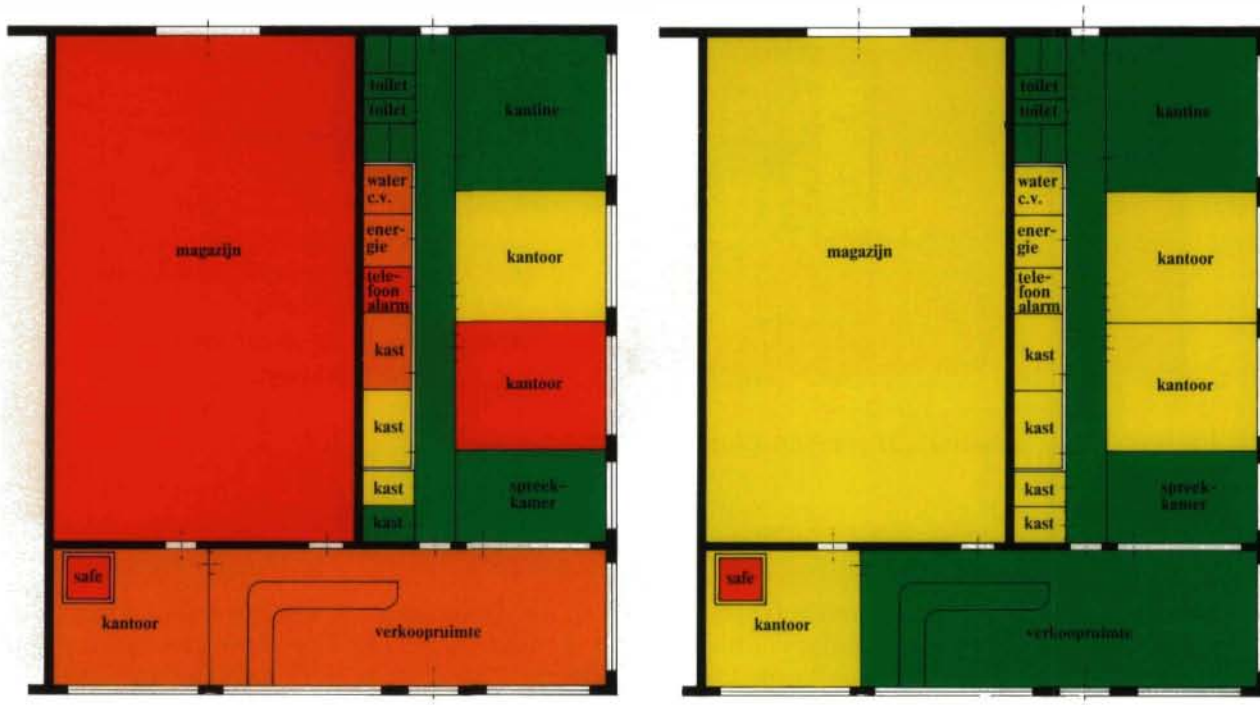
Beveiligingsplattegrond: bestaande drempels

In het beveiligingstraject worden de bouwkundige, elektronische en overige (portier, en dergelijke) beveiligingsmiddelen op de plattegrond van het gebouw in beeld gebracht. De afzonderlijke ruimtes van het gebouw worden gekleurd, waarbij de toegepaste kleur afhankelijk is van de relatieve mate van beveiliging die voor deze ruimte (of delen van die ruimte, bijv. een kluis) geldt. Meestal zal dit beveiligingsniveau van ruimtes gemeten kunnen worden in termen van **toegankelijkheid** van die ruimte: hoeveel mensen (en welke mensen: eigen werknemers, mensen van buitenaf) kunnen zich makkelijk toegang verschaffen tot die ruimte?

Op de beveiligingsplattegrond betekenen de 4 kleuren het volgende:

rood	zeer hoge drempel
oranje	hoge drempel
geel	drempel
groen	geen drempel

De beveiligingsplattegrond geeft inzicht hoe goed de verschillende ruimtes binnen het gebouw beveiligd zijn. Het geeft ook meteen een indruk van de onderlinge samenhang in de beveiliging: zo is het meestal beter als een rode ruimte (zwaar beveiligd) niet direct grenst aan een groene ruimte (niet/nauwelijks beveiligd).



Figuur 4: bedrijfsprocessen-plattegrond

beveiligingsplattegrond

In figuur 4 zijn de bedrijfsprocessen- (links) en de beveiligingsplattegrond (rechts) afgebeeld van een groothandel in meetinstrumenten. Met andere woorden: links is aangegeven hoe kwetsbaar de verschillende ruimtes zijn en rechts de toegankelijkheid van de verschillende ruimtes.

Risico-analyse: combinatie van de bedrijfsprocessen- en beveiligingsplattegrond

Vergelijking van de twee plattegronden geeft bij kleurverschillen op (onderdelen van) de plattegrond een risico weer en geeft daarmee een aanzet voor de risico-analyse. Met name de plaatsen waar de kleurverschillen groot zijn verdienen extra aandacht, bijvoorbeeld rode voorwerpen (zeer kwetsbare/aantrekkelijke spullen) in een voor publiek toegankelijke (=

groene) ruimte. Of andersom, een stapel folders die in de kluis bewaard worden (groene voorwerpen in een rode ruimte). Op het eerste gezicht lijkt dit laatste voorbeeld niet zo alarmerend, maar het kan wel als consequentie hebben dat de kluis vaker open moet dan strikt noodzakelijk is, bovendien wordt de aanwezige beveiliging op een onrendabele manier benut. De risico-analyse spitst zich toe op twee vragen:

- Worden de aanwezige drempels in het gebouw in relatie tot de lokatie en routing van de kwetsbaarheden goed benut (kleurverschillen?)
- Zijn de drempels hoog genoeg in relatie tot de mate van kwetsbaarheid?

Gevonden kleurverschillen worden daarbij als volgt geïnterpreteerd:

		bedrijfsprocessen-plattegrond			
		groen	geel	oranje	rood
beveiligings- plattegrond	groen	O.K.	te laag beveiligd/		
	geel		O.K.	aandachtspunt	
	oranje	oneconomische		O.K.	
	rood	beveiliging			O.K.

Bij het zoeken naar **oplossingen** kan men twee kanten op:

- Aanpassen van bedrijfsprocessen aan de bestaande beveiligingssituatie: men gaat dan bepaalde goederen(stromen) of activiteiten verplaatsen naar ruimten met een bijpassend beveiligingsniveau. Rode spullen komen in rode ruimtes, groene spullen in groene ruimtes.
- Aanpassen van het beveiligingsniveau aan de bedrijfsprocessen: men laat de goederen(stroom) en de activiteiten waar ze zijn, en men past de beveiliging aan (verhogen of verlagen).

De oplossing die men vindt kan heel goed bestaan uit een mix van deze beide benaderingen. In de praktijk zijn er natuurlijk altijd grenzen aan de mogelijkheid om bedrijfsprocessen en -goederen te verplaatsen (de nieuwe indeling moet wel werkbaar blijven voor het personeel) en aan de mogelijkheid om bepaalde bedrijfsruimten te beveiligen (sommige ruimten moeten nu eenmaal zeer toegankelijk zijn).

Het verdient aanbeveling om de gevonden oplossingen weer uit te zetten op twee plattegronden: zo kan men direct aanschouwelijk maken of de nieuwe situatie inderdaad een verbetering is. Mogelijk vindt men nieuwe knelpunten, die weer om een oplossing vragen.

3.2 De wielenmethode

De wielenmethode is wat abstracter dan de kleurenmethode maar heeft als voordeel dat alle 4 beveiligingsniveaus, dus ook het hogere niveau van de bedrijfsvoering, voldoende aandacht krijgen.

Het gebruik van de wielenmethode zorgt ervoor dat men het probleem van de bedrijfsbeveiliging eerst in zijn volle breedte moet bekijken, waarmee wordt voorkomen dat men te snel doorschiet naar oplossingen van deelproblemen (stokpaardjes). De 'wielen' worden daarbij gebruikt als aandachtverdelers, een beetje vergelijkbaar met de bekende 'schijf van vijf' uit de voedingsleer.

Ook bij de wielenmethode wordt uitgegaan van de twee bekende trajecten (bedrijfsvoering respectievelijk beveiliging), die in samenhang met elkaar bekeken moeten worden. Om dit te realiseren zijn er twee 'wielen' ontworpen: het 'bedrijfsvoeringswiel' en het 'beveiligingswiel'. Beide wielen zijn opgedeeld in 4 segmenten die min of meer corresponderen met de 4 beveiligingsniveaus. Bij elk segment hoort een reeks van vragen, die voor het inventariseren van de huidige bedrijfsvoering en beveiliging van belang zijn. Elk wiel is dan ook eigenlijk niet meer of minder dan een checklist. Door de vragen uit de checklist te beantwoorden komt men op ideeën, randvoorwaarden of anderszins diepe gedachten die relevant zijn voor het concrete beveiligingsvraagstuk dat men onder handen heeft. Elk wielsegment kan bijdragen aan een situatie die veiliger is.

Uiteindelijk moeten de twee wielen als raderen in elkaar grijpen, waarbij het ene rad als het ware linksom draait (top-down) en het andere rechtsom (bottom-up).

De vragen vanuit het bedrijfsvoeringswiel dalen af van niveau 4 (bedrijfsvoering) naar niveau 1 (middelen), terwijl de vragen vanuit het beveiligingswiel juist oplopen vanuit niveau 1 (delicten/risico's) naar niveau 4 (beveiligingsbeleid).



Figuur 5: het bedrijfsvoeringswiel

**vragen vanuit het bedrijfsvoeringswiel
(TOP DOWN)**

Beleid:

- 1 Wat zijn de hoofddoelen van de organisatie?
- 2 Op welke wijze worden deze doelen verwezenlijkt (hoofdfuncties/bedrijfsprocessen)?
- 3 Wie zijn de belangrijkste klanten?

Cultuur c.q. risico-bewustzijn:

- 1 Wat wordt er binnen de organisatie gedaan aan deskundigheidsbevordering en voorlichting over criminaliteitspreventie?
- 2 Hoe is de preventiehouding van de mensen binnen de organisatie (top-middenkader-uitvoering)?
 - wordt erover gepraat
 - is men alert
 - zijn medewerkers op de hoogte van de organisatie van de beveiliging en de beveiligingsmaatregelen?
- 3 Wordt de preventie-houding van de medewerkers meegenomen in functioneringsgesprekken?

Functioneren van de organisatie:

- 1 Hoe is de organisatie gestructureerd?
- 2 Welke processen en procedures voltrekken zich binnen de organisatie?
- 3 Welke processtromen spelen hierbij een rol, hoe en waar lopen deze stromen? (goederen/geld/informatie/mensen)
- 4 Wat is de waarde van de goederen en informatie voor de organisatie?
- 5 Wat is de waarde van de goederen en informatie voor kwaadwillende?
- 6 Hoe verschillen deze stromen in de dag- en nachtsituatie?

Hulpmiddelen bij de bedrijfsuitoefening:

- 1 Welke waardevolle of cruciale hulpmiddelen zijn er binnen de organisatie aanwezig om de processtromen gaande te houden?
- 2 Wat is de lokatie van deze hulpmiddelen en wat is het verschil in de dag- en nachtsituatie?



Figuur 6: het beveiligingswiel

**vragen vanuit het beveiligingswiel
(BOTTOM UP)**

Delicten/risico's:

- 1 Door welke delicten is de organisatie in de afgelopen jaren getroffen?
- 2 Welke delicten zijn in de directe omgeving van de organisatie gepleegd als gevolg van (de aanwezigheid van) die organisatie?
- 3 Zijn de kenmerken/achtergronden van deze delicten bekend? (daders, werkwijze, plek, tijd, schade ?)
- 4 Overige criminele risico's?
- 5 Wordt de top hierover geïnformeerd en hoe?

Beveiligingsmiddelen:

- 1 Welke beveiligingsmiddelen zijn toegepast?
- 2 Op welke plaatsen zijn deze middelen ingezet?
- 3 Wat is de kwaliteit van de toegepaste middelen (normen/certificering)?
- 4 In welke configuratie zijn deze middelen toegepast?
- 5 Wat is het verschil in dag- en nachtsituatie?

Functioneren van de beveiliging:

- 1 Wat is de plaats van de beveiligingsafdeling binnen de organisatiestructuur?
- 2 Hoe is de beveiliging georganiseerd binnen de organisatie?
- 3 Welke organisatorische maatregelen zijn er getroffen?
- 4 Zijn er voor de medewerkers voorschriften of handleidingen gemaakt voor het gebruik en onderhoud van de aanwezige beveiligingsmiddelen en -systemen?
- 5 Bestaat er een informatie-netwerk binnen de organisatie voor het melden van onregelmatigheden?
- 6 Hoe wordt er omgegaan met onregelmatigheden?
- 7 Is er nazorg voor slachtoffers van incidenten?

Beveiligingsbeleid:

- 1 Is er beleid ten aanzien van beveiliging?
- 2 Wat zijn de hoofddoelstellingen van dit beleid?
- 3 Is dit beleid verwoord in een beveiligingsplan?
- 4 Is er een duidelijke relatie tot de hoofddoelen van de organisatie?

De hier gepresenteerde vragenlijsten zijn beperkt tot de hoofdzaken, de lijsten kunnen uiteraard verder aangevuld en verfijnd worden.

3.3 De twee methoden samengevoegd tot een plan van aanpak

Toepassing van de twee methoden maakt nog geen beveiligingsbeleid. Daartoe moeten de twee methoden worden ingebed in een plan van aanpak. De belangrijkste kenmerken van een goed plan van aanpak voor bedrijfsbeveiliging zijn:

- 1 er moet aan **alle vier niveaus** voldoende **aandacht** besteed worden;
- 2 er moet in het plan van aanpak een duidelijke **afstemming** plaatsvinden **tussen** de 4 niveaus onderling;
- 3 beveiliging wordt bekeken vanuit de **twee trajecten** (bedrijfsvoering en beveiliging);
- 4 en de uitkomsten van beide trajecten moeten goed op elkaar **afgestemd** zijn.

Zoals we zagen zijn de twee gepresenteerde methoden (kleuren en wielen) belangrijke hulpmiddelen om te komen tot een plan van aanpak dat aan de hier genoemde eisen voldoet. Als de twee methoden goed worden toegepast beschikt men over een degelijk ontwerp voor een beveiligingslimousine. Daarbij is het wel van belang dat men de onderdelen in de goede volgorde in elkaar zet. Dit kan men doen door de methoden toe te passen in een **stapsgewijs plan van aanpak**, dat er als volgt uit kan zien:

stap 1 inventarisatie met behulp van de wielenmethode

stap 2 risico-analyse met behulp van de kleurenmethode

stap 3 ontwerpen van maatregelen

stap 4 evalueren van de maatregelen met behulp van de kleurenmethode

stap 1: inventarisatie met behulp van de wielenmethode

Met behulp van het **bedrijfsvoeringswiel** wordt allereerst bepaald wat de belangrijkste doelen en processen van de organisatie zijn (de 'core business'). Op basis daarvan kunnen de belangrijkste kwetsbaarheden in de bedrijfsprocessen worden aangegeven: welke goederen, middelen en activiteiten zijn essentieel voor het functioneren van de organisatie? De exacte fysieke lokatie of routing van deze kwetsbaarheden, en de (fysieke) beveiliging daarvan wordt nog even buiten beschouwing gelaten: dat wordt in stap 2 met kleur in kaart gebracht.

Met behulp van het **beveiligingswiel** wordt de totale beveiliging geïnventariseerd, met speciale aandacht voor de beleidsmatige en functionele inbedding van beveiliging in de totale bedrijfsvoering. Het gaat dan om vragen als: is er een beveiligingsplan? wat zijn de doelen daarvan? sporen de beveiligingsdoelen met de bredere bedrijfsdoelen? (is de beveiliging gericht op die kwetsbaarheden die vanuit de bedrijfsvoering gezien essentieel zijn?), maakt beveiliging/preventie onderdeel uit van de bedrijfscultuur? hoe dan? etc.

De fysiek aanwezige beveiliging (lagere niveaus) wordt in stap 2 met kleuren in kaart gebracht.

stap 2: risico-analyse met behulp van de kleurenmethode

Met behulp van de kleurenmethode wordt in kaart gebracht wat de lokatie en routing is van de in stap 1 (bedrijfsvoeringswiel) bepaalde kwetsbaarheden: de bedrijfsprocessenplattegrond. Daarnaast brengt men de bestaande beveiliging in kaart: de beveiligingsplattegrond.

Door het vergelijken van beide plattegronden maakt men vervolgens een risico-analyse, door die plekken en routes te benoemen waar kleurverschillen optreden.

stap 3: ontwerpen van maatregelen

Na de risico-analyse gaan de trajecten weer uit elkaar.

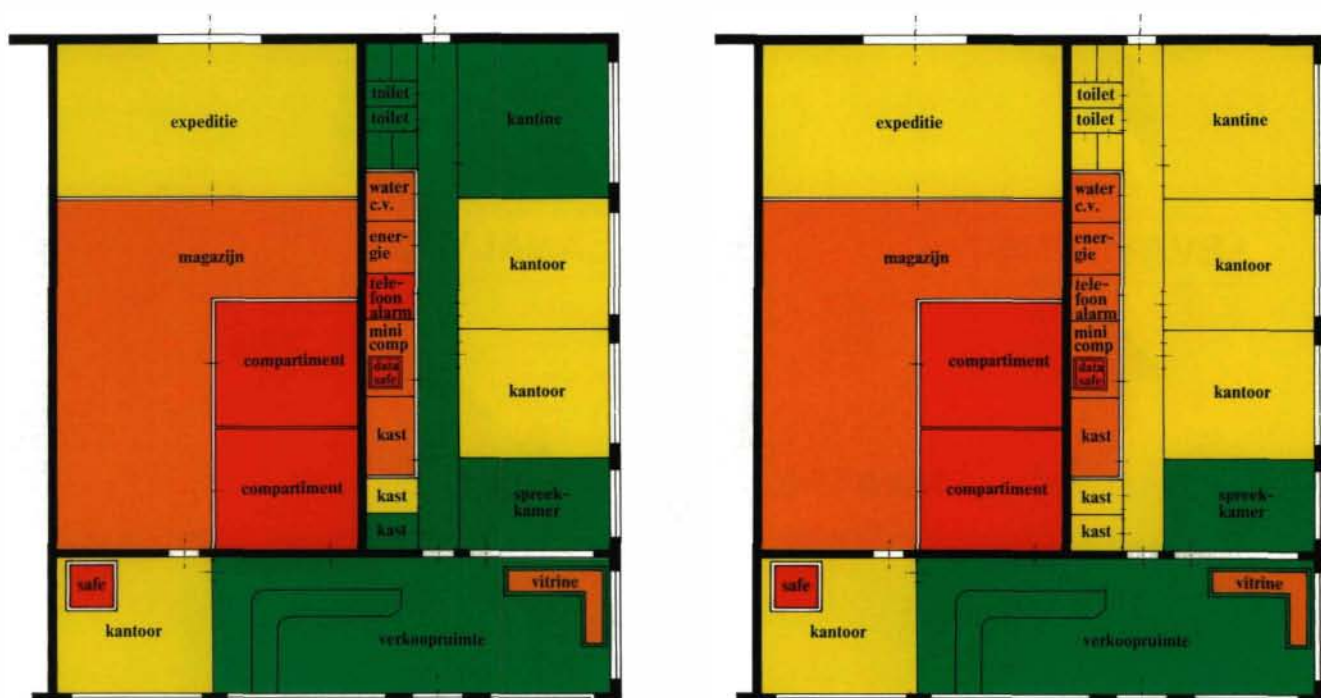
In het **bedrijfsvoeringstraject** wordt onderzocht op welke wijze het risico-bewustzijn verhoogd kan worden en of bepaalde bedrijfsprocessen kunnen worden aangepast teneinde de kwetsbaarheid van de organisatie te verlagen. Tevens wordt vastgesteld welke grenzen er aan de fysieke beveiliging gesteld moeten worden: hoe ver kan beveiliging gaan zonder het functioneren van de organisatie te belemmeren?

Het bedrijfsvoeringstraject wordt als eerste doorlopen omdat:

- de noodzaak voor fysieke beveiliging door maatregelen op het bedrijfsvoeringsniveau kan worden verlaagd;
- hier de 'beveiligingsgrenzen' worden vastgesteld.

In het **beveiligingstraject** wordt gezocht naar oplossingen die passen bij de in stap 2 vastgestelde risico's. Al eerder werd gezegd dat oplossingen twee kanten op kunnen gaan: aanpassingen in de bedrijfsvoering en aanpassingen in de beveiliging. Vanuit het bedrijfsvoeringstraject is inmiddels duidelijk geworden waar de mogelijkheden en grenzen liggen wat betreft de aanpassingen in de bedrijfsvoering.

Er kan nu gericht gekeken worden waar en op welke wijze beveiligingsdrempels moeten worden aangebracht, verhoogd of verlaagd.



Figuur 7: bedrijfsprocessen-plattegrond

beveiligingsplattegrond

In de bovenstaande figuur is de gewijzigde situatie afgebeeld van een groothandel in meetinstrumenten (zie ook figuur 3 en 4). De indeling en inrichting van het magazijn is drastisch gewijzigd. Van het magazijn is een expeditieruimte afgescheiden. De toegankelijkheid van het magazijn is hiermee verlaagd. Tevens zijn er twee bouwkundig verstevigde compartimenten in het magazijn gebouwd, waarin de kostbare meetinstrumenten van het assortiment bewaard worden. De mini-computer is verplaatst van het kantoor naar een beveiligde kast. In de verkoopruimte is een beveiligde vitrine geplaatst waarin de showmodellen geëxposeerd worden.

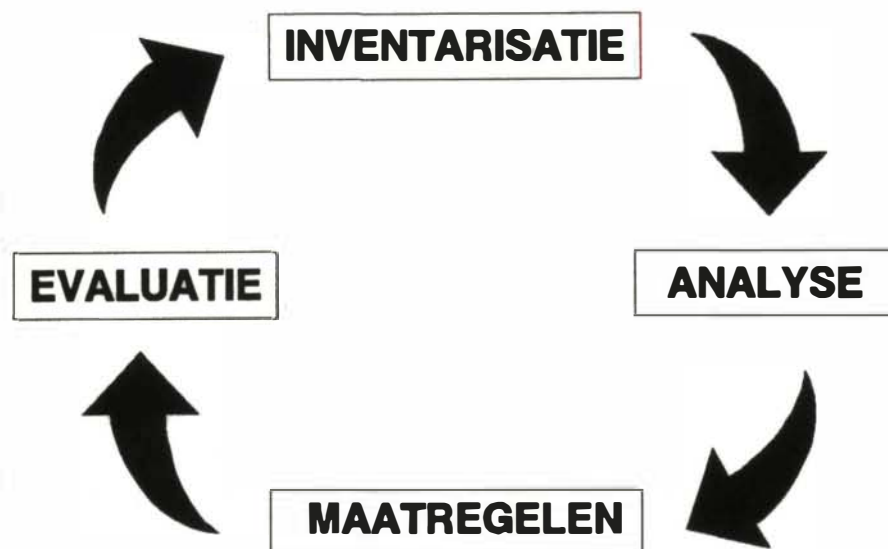
stap 4: evalueren van de maatregelen met de kleurenmethode

De voorgestelde wijzigingen in de beveiliging en de bedrijfsprocessen worden opnieuw met kleur in kaart gebracht. Gecontroleerd wordt of alle risico's nu in voldoende mate gedekt zijn. Wellicht ontstaan er nieuwe knelpunten, die eerst opgelost moeten worden. Dan moet stap 3 net zo lang herhaald worden totdat het resultaat naar ieders tevredenheid kan worden uitgevoerd.

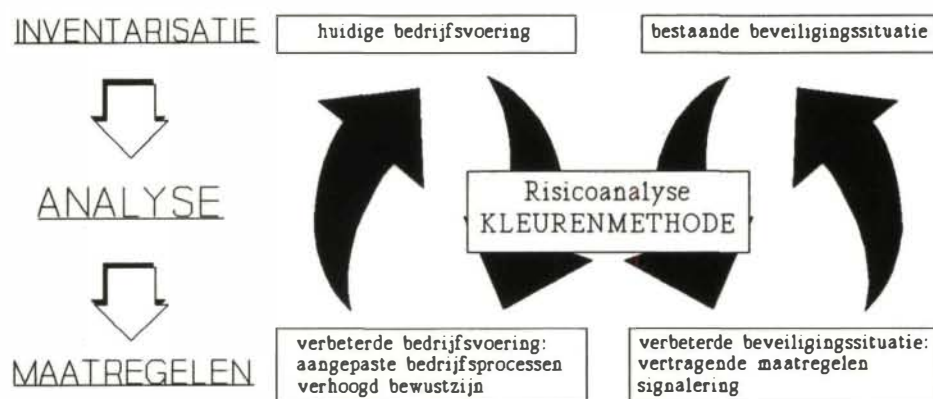
tot slot

Na invoering van de maatregelen kan de nieuwe situatie (een aangepaste bedrijfsvoering en een verbeterde beveiligingssituatie) opnieuw geïnventariseerd en geanalyseerd worden. De resultaten hiervan kunnen wederom aanleiding geven tot het treffen van maatregelen. Het beveiligingsproces binnen deze aanpak is continue en cyclisch. Op deze wijze ontstaat een opwaartse spiraal: beveiliging wordt steeds verder geïntegreerd in de totale bedrijfsvoering, waarbij ook de bedrijfsprocessen bij de beveiligingsproblematiek wordt betrokken.

Een en ander is in de figuren 8 en 9 weergegeven.



figuur 8: basiscyclus



figuur 9: globale opzet

Literatuur

- Claes, P.F. en H.J.J.M. Meerman. Risk Management, inleiding tot het risicobeheersproces. Stenfert Kroese, Leiden/Antwerpen, 1991.
- Beveiliging van gebouwen deel 4: Kantoren. P. van Soomeren en H. Stienstra; november 1989.
Stichting Bouwresearch, Postbus 20740, 3001 JA Rotterdam. Tel.: 010-4117276 /4123528.
Publicatienummer 205.
- Beveiliging van gebouwen deel 5: Bedrijfsgebouwen/terreinen. P. van Soomeren en H. Stienstra; februari 1990.
Stichting Bouwresearch, Postbus 20740, 3001 JA Rotterdam. Tel.: 010-4117276/4123528.
Publicatienummer 210.
- Handleiding Criminaliteitsbeheersing.VNO; februari 1990.
Verbond van Nederlandse Ondernemingen, Postbus 93093, 2509 AB 's-Gravenhage. Tel.: 070-3497373.
- Poly-beveiligingszakboekje. L.J. van Aart e.a.; 1990.
Koninklijke PBNA b.v., Postbus 9053, 6800 GS Arnhem. Tel.: 085-575911

Adressen

(normen hang- en sluitwerk:)
Nederland Normalisatie Instituut (NNI)
Postbus 5059
2600 BG Delft
tel. 015 - 690390

Stichting Slotencertificaat
Postbus 54
3740 AB Baarn
tel. 02154 - 21380

Colofon

Deze brochure is een uitgave van het Bureau Landelijk Coördinator Voorkoming Misdrijven. 's Gravenhage, oktober 1992.

De in deze brochure beschreven methodieken zijn in de afgelopen jaren ontwikkeld door de organisatie Voorkoming Misdrijven. Medewerking werd verleend door CIVI Consultancy (Leidschendam) Bureau Damhuis Elshout Verschure ('s-Hertogenbosch) en Van Dijk, Van Soomeren en Partners BV (Amsterdam).

Als gevolg van de reorganisatie van de Nederlandse politie wordt het Landelijk Bureau Voorkoming Misdrijven per 1 januari 1993 opgeheven. Op het moment van het verschijnen van deze brochure is nog niet geheel duidelijk op welke wijze de criminaliteitspreventie binnen de nieuwe regionale politiekorpsen organisatorisch wordt vormgegeven. Het is daarom helaas niet mogelijk in deze brochure aan te geven bij wie u, na de reorganisatie van de politie, aan het juiste adres bent voor aanvullende adviezen.