



stichting **b**ouw **r**esearch

beveiliging van gebouwen deel 4 kantoren

In de reeks Beveiliging van gebouwen zijn reeds verschenen:

Deel 1: Eengezinswoningen, SBR-publikatie 160

Deel 2: Meergezinswoningen, SBR-publikatie 170

Deel 3: Winkels, SBR-publikatie 180

In voorbereiding is:

Deel 5: Bedrijfsgebouwen/terreinen

rapporteurs:

P. van Soomen

H. Stienstra

Bureau Criminaliteitspreventie



Stichting bouwresearch

**beveiliging van
gebouwen
deel 4
kantoren**

Rotterdam, 1989

De stichting stelt zich ten doel:

- a. in de bouwnijverheid produktiviteit en kwaliteit te verhogen, en de continuïteit in de werkgelegenheid te bevorderen;
- b. de kennis op het terrein van de bouwnijverheid te vergroten en te verspreiden naar en binnen alle organisaties waarmee de stichting een relatie onderhoudt;
- c. voorts al hetgeen dat met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting en degenen die aan deze publikatie hebben medegewerkt, hebben een zo groot mogelijke zorgvuldigheid betracht bij het verwerken – volgens de huidige stand van wetenschap en techniek – van de in deze publikatie vervatte gegevens. Nochtans moet de mogelijkheid dat zich toch onjuistheden in deze publikatie zouden bevinden niet worden uitgesloten. Degene die van deze publikatie gebruik maakt, aanvaardt daarvoor het risico. De stichting sluit, mede ten behoeve van degenen die aan deze publikatie hebben meegewerkt, iedere aansprakelijkheid uit voor schade die mocht voortvloeien uit het gebruik van informatie in deze publikatie.

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze ook, zonder voorafgaande schriftelijke toestemming van de Stichting Bouwresearch.

No part of this book may be reproduced in any form by print, photoprint, microfilm or any other means without written permission from the Stichting Bouwresearch.

<i>Woord vooraf</i>	7	5 Ruimte-risico-inschattingsmodel (RRIM)	(39–42)
<i>Samenvatting</i>	9	Algemeen	39
<i>Summary</i>	13	Het RRIM	39
1 Inleiding	(16–22)	6 RRIM per ruimte/element	(43–51)
Algemeen	17	Algemeen	43
– inbraakbeveiliging	19	RRIM per ruimte/element	43
– toegangscontrole	19	– toegangen	43
– leeswijzer	20	– verkeersruimten en trappehuizen	44
2 Definitie kantoorgebouwen	(21–26)	– nooduitgangen en noodtrappehuizen	44
Algemeen	21	– kelders	46
– grootte	21	– technische ruimten	46
– locatie	21	– leidingkokers	46
– publiek	22	– magazijnen en archieven	47
– ondersteuning	23	– postkamer en expeditie	47
– specifiek	23	– kluizen	47
Trends, prijs en afnemers	24	– computerruimten	47
– aanbod-trend	24	– bewakingsruimten	48
– opname-trend	24	– schoonmaakruimten	48
– prijs	26	– kantoorruimten	49
– afnemers naar type gebruikers	26	– publieksruimten	49
3 Omschrijving risico's	(27–34)	– kantine en recreatieve ruimten	49
Algemeen	27	– gevels	49
Risico's kantoorgebouwen	28	– daken	50
– algemeen	28	– terreinen	51
– welke delicten / welke schade	28	7 Inbraakbeveiliging	(52–65)
Vandalisme	29	Algemeen	53
Inbraak	30	Gevels, kozijnen, ramen en deuren	53
Brandstichting	32	– gevels	53
Overige risico's	33	– kozijnen, ramen en deuren	54
4 Beveiligingsplan	(35–38)	Hang- en sluitwerk	55
Algemeen	35	Glas en glasafscherming	56
Inventarisatie en definities van de risico's	36	– glas	56
Definitie van gebieden	36	– glasafscherming	57
Definitie van beveiliging	36	– kogelwering	57
Bezwaren	37	Daken en vluchtwegen	59
Gebruiksvriendelijkheid	37	– lichtkocpels en dergelijke	60
Controle en onderhoud	37	– dakmateriaal	61
En nu ... ?	37	– vluchtwegen	61
		Inbraaksigaleringsystemen	62
		– functie	62
		– werking	62
		– installatie	63
		– de bouwkundig ontwerper	64

(zie verder)

8 Compartmenteren	(66–85)	10 Toegangscontrole in bouwkundig detail	(96–115)
Algemeen	67	Algemeen	97
Computerruimten	67	De kaartlezer	97
– risico's en ligging	68	Het deurconcept	98
– het gebouw	68	Deuren in kantoren	98
– toegangscontrole	68	– speciale 'sluisdeuren'	100
– data-archiefruimten	69	– sabotage	102
Archiefruimten	69	– overige in- en uitgangen	103
– traditionele archiefruimten	69	– draairichting	104
– data-archieven	69	– automatische deuren en aandrijvingen	104
– VDMA-normen	70	Speciaal hang- en sluitwerk	106
– datakluisen	71	– sloten en sluitsystemen	106
Kluisruimten	73	– mechanische codesloten	107
– eisen voor de ghele kluis	74	– elektrische deurgrendels	107
– eisen voor de kluiswanden, vloer en plafond	75	– elektrische deuropeners	107
– veiligheidsmaatregelen tijdens de bouw	75	– elektromotorsloten	111
Brand- en inbraakwerende kasten	76	– elektromagnetische deurvergrendelingen	111
– constructie van brandwerende kasten	78	– deursluiters – deuropeners	111
– constructie van datasafes en diskettensafes	78	– paniekopeners	112
– constructies van brandkasten, inbraakwerende kasten en (inbouw)kluisen	78	– automatische kantschuif en deurselector	113
– inbouwkluisen	79	– bedieningspanelen	114
– eisen te stellen aan brandkasten en inbraakwerende kasten	82	Deurenboek	114
Ruimten voor geldzaken	82	11 Terreinbeveiliging	(116–122)
– Intern en extern geldtransport	84	Algemeen	117
Bewakingsruimten	84	Afscheidingen	117
– meldkamer	84	– natuurlijke afscheidingen	117
– portiersloge	85	– technische afscheidingen	118
– ruimten voor bewakingspersoneel	85	Poorten en obstakels	119
9 Toegangscontrole	(86–95)	Controle	120
Algemeen	87	Parkeerplaatsen	120
Toegangscontrole	87	Verlichting	120
Sloten en sleuteldiscipline	88	Gesloten televisiesystemen	121
Sloten zonder sleutel	88	Bewakingsruimten	122
Sloten met kaarten	90	12 Vandalisme	(123–129)
Persoonsgebonden toegangscontrole	91	Algemeen	123
Complete toegangscontrole	91	– wat is vandalisme?	123
De toekomst	93	Cijfers en gegevens over vandalisme	123
Ontwerp	95	– privé-bezit	123
– nadruk op bouwkundige details	95	– (semi-)openbaar bezit	125
		– bedrijfsbezit	125
		Preventie bij kantoorgebouwen	127

(zie verder)

<i>Literatuur</i>	131
-------------------	-----

<i>Bijlagen</i>	(133–140)
-----------------	------------

1 Inhoudsopgaven deel 1, 2, 3 en 5

Deel 1: Eengezinswoningen	133
Deel 2: Meergezinswoningen	134
Deel 3: Winkels	135
Deel 5: Bedrijfsgebouwen/terreinen	137

2 Organisaties en instellingen 139

<i>Colofon</i>	141
----------------	-----

De veelvuldig voorkomende vernielingen aan en inbraken in gebouwen vragen reeds in de ontwerpfase, en zelfs daarvoor, de aandacht van opdrachtgevers, ontwerpers en toekomstige gebruikers. Door vroegtijdig een analyse te maken van de risico's die het gebruik van een gebouw in de gebruikperiode met zich meebrengt, kan worden voorkomen dat gebouwen naderhand een bron van ergernis worden omdat ze te gemakkelijk doelwit van ongewenste gasten zijn geworden. Met de gegevens van die analyse kan de ontwerper rekening houden bij de situering.

Vooraf ook in de preventieve sfeer kunnen technische maatregelen en middelen van voldoende kwaliteit worden toegepast om de kans op inbraak en vandalisme te beperken. Tot dit laatste draagt ook de juiste keuze van materialen en de wijze van verwerking daarvan bij. De studiegcommissie C-40 (Beveiliging van gebouwen) heeft zich tot doel gesteld een serie goed gedocumenteerde rapporten over deze onderwerpen op te stellen voor opdrachtgevers en ontwerpers, steeds gericht op de meest voorkomende typen gebouwen.

Dit rapport over kantoren is het vierde deel in deze serie.

Het eerste deel, dat eengezinswoningen behandelde, verscheen in december 1987. Hierna volgde het tweede deel, meergezinswoningen, en een derde deel over winkels.

In deze reeks zullen nog de volgende delen uitkomen:

- deel 5: Bedrijfsgebouwen/terreinen;
- deel 6: Scholen.

De commissie hoopt dat deze rapporten een bijdrage zullen leveren aan het op rationele wijze beveiligen van gebouwen.

ir. P. van der Heiden,
voorzitter studiegcommissie C-40

Dit vierde deel in de reeks Beveiliging van gebouwen is een leidraad voor het bouwtechnisch beveiligen van kantoorgebouwen tegen de meest voorkomende risico's van criminaliteit.

Allereerst wordt in *hoofdstuk 1* aangetoond hoe belangrijk het is om het ontwerp beveiliging reeds in het ontwerp van een kantoorgebouw mee te nemen. Met de stijgende criminaliteit is beveiliging geen luxe. Als men rekening houdt met die beveiliging in het ontwerp van een kantoorgebouw, levert dat in de exploitatie (beheers)fase zeker zijn rendement op.

Vervolgens worden in dit eerste hoofdstuk een zestal wegen geschetst die gevolgd kunnen worden bij het bouwtechnisch beveiligen tegen inbraak alsmede zes manieren om toegangscontrole te regelen.

In *hoofdstuk 2* wordt eerst een algemene omschrijving gegeven van wat men onder het begrip kantoorgebouw moet verstaan. Vervolgens worden enkele kerngetallen over de kantorenmarkt gepresenteerd. Zowel het aanbod als het aantal transacties blijkt flink toegenomen te zijn en dat is een trend die in de komende jaren zeker door zal zetten. Andere kerngetallen die gepresenteerd worden betreffen de prijzen, de geografische spreiding en het type afnemers op de kantorenmarkt.

Hoofdstuk 3 geeft een omschrijving van de criminele risico's waar men bij kantoorgebouwen rekening mee moet houden. Over dit onderwerp blijkt nauwelijks informatie te bestaan. Het zeer schaarse materiaal dat enig inzicht geeft in de schade ten gevolge van criminaliteit duidt erop dat de delicten inbraak, vandalisme en brandstichting de belangrijkste risico's lijken. Deze risico's worden vervolgens kort behandeld.

In *hoofdstuk 4* wordt ingegaan op het ontwerp beveiligingsplan. In essentie gaat het er daarbij om dat reeds in een zeer vroeg stadium van het ontwerpproces de

voor het desbetreffende kantoorgebouw relevante risico's geïdentificeerd en geanalyseerd worden, waarna de tegenmaatregelen uitgestippeld kunnen worden.

Het is daarbij een keiharde randvoorwaarde dat beveiligingsmaatregelen in kantoren niet haaks mogen staan op de dagelijkse menselijke routine in kantoren. Omdat niet alleen investeringskosten maar ook exploitatiekosten gedurende het ontwerp- en bouwproces snel aan beïnvloedbaarheid inboeten (met de keuze van een ontwerp is 55% van de exploitatiekosten vastgelegd), is het van belang het beveiligingsplan al in het programma van eisen mee te nemen.

Aangezien over het algemeen de vereiste beveiligingsgraad per ruimte in het gebouw verschilt, zal men zowel de risico's als de beveiligingsmaatregelen per ruimte/gebied moeten definiëren.

Hiervoor wordt in *hoofdstuk 5* een praktisch hulpmiddel aangereikt: het Ruimterisico-inschattingmodel (RRIM). In dat model – waarvan een voorbeeld is opgenomen – kan men per ruimte de mogelijke risico's invullen. Daarachter vult men de kans in dat genoemd risico echt plaatsvindt en de ernst van de gevolgen.

Op grond van deze inschattingen, die noodgedwongen vaak subjectief zullen zijn, kan men tenminste prioriteiten bepalen en een (beveiligings)beleid uitstippelen. Kortom: met het RRIM kunnen opdrachtgever en ontwerper komen tot een rationeel beveiligingsplan dat in het verdere ontwerpproces meegenomen kan worden.

Als ondersteuning bij de invulling van het RRIM worden in *hoofdstuk 6* een kleine twintigtypen ruimten die men in een kantoor kan aantreffen behandeld (van kantine tot leidingkoker). Per ruimte worden enkele uit beveiligingsoogpunt essentiële zaken kort aangestipt waarna vervolgens een verwijzing wordt gegeven naar de meer technische detail-hoofdstukken en paragrafen in het vervolg van dit rapport. Dit hoofdstuk vormt daarmee in feite een

scharnierpunt: van risico-inschatting naar de ontwerp-oplossingen.

In *hoofdstuk 7* wordt ingegaan op de beveiliging (met name tegen inbraak) van het gebouw. Daarbij wordt allereerst de bouwkundige schil van het gebouw onder de loep genomen. De eisen die uit inbraakpreventief oogpunt moeten worden gesteld aan gevels, kozijnen, ramen en deuren passeren de revue. Vervolgens wordt aandacht besteed aan het hang- en sluitwerk (de bestaande NEN-normen), aan glas en glasafscherming en aan de qua beveiligingsproblematiek vaak onderschatte daken en vluchtwegen.

Pas als de bouwtechnische beveiliging op niveau gebracht is, kan men zich op de aanvullende elektronica richten. De laatste paragraaf van dit hoofdstuk betreft dan ook de functie, werking en installatie van inbraaksignaleringsystemen in het gebouw.

In *hoofdstuk 8* wordt ingegaan op het onderwerp 'compartimenteren': het van de rest isoleren van de zeer risicovolle plekken in het gebouw en het beter beveiligen van die plekken. Dit is een strategie die al sinds mensenheugenis wordt toegepast door geld in kluisruimten onder te brengen en archieven in archiefruimten.

Aan de orde komen achtereenvolgens de computerruimte, de archiefruimte, de kluisruimte, de brand- en inbraakwerende kasten, de ruimte voor geldzaken en ten slotte de bewakingsruimte. Voor elk van de genoemde compartimenten en/of onderdelen daarvan worden de uit beveiligingsoogpunt te stellen eisen behandeld. Het criminele risico rond elk van de compartimenten kan vrijwel nooit los worden gezien van het brandrisico. Waar nodig wordt dan ook op dit onderwerp kort ingegaan.

Toegangscontrole is het onderwerp dat in *hoofdstuk 9* (in bouwkundig detail ook in *hoofdstuk 10*) centraal staat. Terwijl inbraakbeveiliging zich richt op de beveiliging buiten kantooruren, richt toegangscontrole zich vooral op de beveiliging tijdens werktijd.

Allereerst wordt kort stilgestaan bij enkele vormen van toegangscontrole die in kleinschalige situaties goed toepasbaar zijn: een slot dat moet voorkomen dat een onbevoegde werknemer, bezoeker of derde een gebouw of ruimte betreedt. Ingegaan wordt op cijfercombinatiesloten, druktoetspanelen, sloten met kaarten en persoonsgebonden toegangscontrole. Vervolgens wordt stilgestaan bij de meer uitgebreide toegangscontrole waarbij alle belangrijke deuren in het kantoorgebouw worden bewaakt.

Essentieel voor een goede werking van alle toegangssystemen blijken de bouwkundige details. Daaronder verstaan we hier al datgene wat niet direct aangemerkt kan worden als 'de elektronica'. Dit betreft niet alleen de componenten zoals deuren, sloten, deurdrangers, behuizingen, maar ook de bevestiging daarvan, sparringen, doorvoeren van kabels enz. Dit onderwerp staat centraal in *hoofdstuk 10*: toegangscontrole in bouwkundig detail. Allereerst wordt ingegaan op de kaartlezer.

Voorts worden de meest voorkomende (buiten)deur-situaties behandeld. Daarbij wordt zowel aandacht besteed aan de hoofd-entree-partij als aan de overige in- en uitgangen.

Tevens wordt vrij uitgebreid ingegaan op speciaal hang- en sluitwerk, zoals onder andere mechanische codesloten, elektrische deurgrendels en -openers, elektromotorsloten, elektromagnetische deurgrendelingen en paniekopeners.

Omdat het aantal te beveiligen deuren in een wat groter beveiligingsplan vaak niet gering is en de details per deur veelal verschillen, wordt in de laatste paragraaf van dit hoofdstuk ingegaan op een hulpmiddel dat veel misverstanden en dubbel werk kan voorkomen: de vervaardiging van een deurenboek. Hiervan wordt een voorbeeld gegeven.

Hoofdstuk 11 van dit rapport behandelt het onderwerp terreinbeveiliging. Aan de orde komen (natuurlijke en technische) afscheidingen, poorten en obstakels, con-

■

trole, parkeerplaatsen, verlichting, gesloten televisiesystemen en en bewakingsruimten. Deze onderwerpen worden kort en vrij algemeen besproken. Ze vormen namelijk het zwaartepunt in het volgende deel in de reeks Beveiliging van gebouwen (deel 5: Bedrijfsgebouwen/terreinen).

In *hoofdstuk 12* wordt kort aandacht besteed aan de onderwerpen vandalisme en brandstichting. Er wordt ingegaan op enkele kerngegevens over omvang en achtergronden. Aan het eind van dit hoofdstuk wordt een aantal preventieve tips gegeven.

Dit deel wordt besloten met een overzicht van de gebruikte *literatuur* en twee bijlagen.

In *bijlage 1* treft men de inhoudsopgaven aan van de eerste drie delen die verschenen zijn in de reeks Beveiliging van gebouwen, alsmede de inhoudsopgave van het aankomende deel 5.

Bijlage 2 geeft een overzicht van relevante organisaties en instellingen.

This fourth part in the series Building security is a set of guidelines for applying building technology to office buildings to make them secure against the most frequently occurring criminal risks.

First of all, in *chapter 1*, the importance of including security early in the design of the office building is demonstrated. With the rising tide of crime security is not a luxury. If security is 'built in' to the design profits in the exploitation (management) phase will be more assured. The first chapter then sketches six ways of construction which can be adopted to prevent burglary and six ways of monitoring admission into the building.

Chapter 2 first gives a general description of what should be understood by the term 'office building'. Some basic figures are then given about the Dutch market in office buildings. It appears that both demand and the number of building contracts are growing vigorously and that this is a trend which is certain to continue in the future. Basic figures are also given about prices, geographical distribution and the type of customers in the office market.

Chapter 3 describes the criminal risks which have to be taken into account regarding office buildings.

On this subject however there appears to be very little information. The information which is available indicates that the most important risks are burglary, vandalism and arson. These risks are treated briefly.

Chapter 4 elaborates on a design plan for security. In essence the relevant risks for a particular office building should be identified and analysed very early in the design. The necessary preventive measures can then be planned. A fundamental requirement is that such measures should not interfere with the daily routine of the office. Since both investment and exploitation costs can be

greatly influenced during the design and construction stages (the choice of design fixes 55% of the exploitation costs) it is important to include the security plan in the specifications. In general the required degree of security varies with location within the building and the risks, and therefore the security measures to be taken, must be defined for each specific area.

Chapter 5 gives practical assistance in this respect: a Risk-estimation model is presented. The possible risks for each part of the building can be fed into the model; the chance of the risk occurring and the consequences can then be identified. Based on these forecasts, which of necessity are often subjective, the priorities at least can be determined and a security policy drafted. In short, by using the Risk-estimation model the principal and the designer can develop a rational security plan which can be included in the design process.

To assist users to fill in the Risk-estimation model, *chapter 6* considers twenty different types of areas which can be found within an office. Essential aspects for each type of area are outlined briefly from the point of view of security, and reference is made to the more detailed chapters and paragraphs to be found in the report. Chapter 6 therefore forms, in fact, a link between risk forecasting and the design solution.

Chapter 7 examines the security of the building with particular reference to burglary. The first aspect to be considered is the building envelope. The requirements for walls, door and window frames, windows en doors are reviewed from the point of view of burglary prevention. Attention is then given to hinges and locks — the existing Dutch NEN standards — glass and glass protection and the often underestimated question of roofs and emergency exits. Electronic aspects of security can also be improved and the last paragraph of

chapter 7 considers the function, operation and installation of burglar alarm systems in the buildings.

Chapter 8 goes into 'compartmentation' design: the isolation of the risk areas from the rest of the building and the improvement of the security of these areas. This is a strategy which has been applied since time immemorial for example, putting money in strong rooms and documents in archives. The chapter then deals in sequence with computer areas, archives, strong rooms, fire and burglar proof boxes, ready cash boxes and finally the control room (alarm centre). Security specifications are set for each of the above compartments or components.

Entry to an office building forms the subject of *chapter 9* (construction details are also discussed in chapter 10). It is necessary for the building to be burglar proof outside office hours. On the other hand entry and exit have to be controlled during working time especially. With all forms of entry control the very first priority is a brief restraint which can be applied easily: a lock which must prevent the entrance of an unauthorized employee, visitor or third party into the building or part of the building. Combination locks, push button panels, card-operated locks and person-related systems of entry control are discussed. The chapter then treats more extensive entry controls in which all important doors to the office building are guarded.

Proper construction details appear to be essential for the correct functioning of all entry control systems. By construction details we mean all that which cannot be directly considered as 'electronics'. This applies both to components such as doors, locks, door levers, (lock) housings, and also the way in which such components are installed. The design forms the subject of *chapter 10*: Entry control — construction details. First of all the chapter discusses the card reader. Consideration is also given to the main

entrance and other entrances and exits. The chapter discusses fairly extensively special types of hinges and lock fittings, such as, coded locks, electrically operated bolts and door opening systems, electric locks, electromagnetic bolts and emergency openers. Because of the number of doors to made secure, and because the security plan is often very comprehensive and the details per door can differ, the last paragraph of this chapter discusses an essential item for preventing misunderstandings and double work: the preparation of a door book. An example of a page in such a book is given.

Chapter 11 of this report treats the subject of terrain security, discussing natural and technical boundaries, gateways and obstacles, control points, parking areas, lighting, close-circuit television systems and monitoring rooms. These subjects are discussed briefly and fairly generally and form the main items in part 5, Buildings/ terrain of the series Building security.

Chapter 12 briefly considers the subjects of vandalism and arson and presents basic data on the magnitude of the problem and the background. The chapter is concluded with a number of tips for their prevention.

This part of the series ends with a literature review and two appendices, the first giving the contents of the first three parts and the next fifth part in the series and which are referred to in the present report, the second summarizes relevant organizations and institutions.

*Verhef het kantoorgebouw
boven z'n risico's*



De beveiliging van kantoren is een combinatie van de fysieke conditie van een gebouw en zijn installaties, de onontbeerlijke instructies aan mensen en de door hen op te brengen discipline.

Allemaal doodnormale zaken waarbij de basis wordt gevormd door het gebouw, de installaties en de inrichting. Precies die zaken waarbij een ontwerper zijn invloed moet aanwenden.

Toegespitst op het onderwerp 'beveiliging tegen criminaliteit' probeert dit rapport hierbij een hulpmiddel te zijn.

Niemand kijkt nog op van het feit dat zaken als hygiëne, brandveiligheid en energie-bezuiniging tegenwoordig automatisch in het ontwerp voor nieuw- of verbouw van een kantoorgebouw worden meegenomen. Dit geldt echter nog nauwelijks voor de beveiliging tegen vandalisme, inbraak en overval op een kantoorgebouw.

Welbeschouwd is het veronachtzamen van het onderwerp beveiliging in het ontwerp een vreemde zaak. Bij het beheer

van kantoorgebouwen is bijvoorbeeld bewaking en toegangsbeheer zeker geen ondergeschikte kostenpost te noemen.

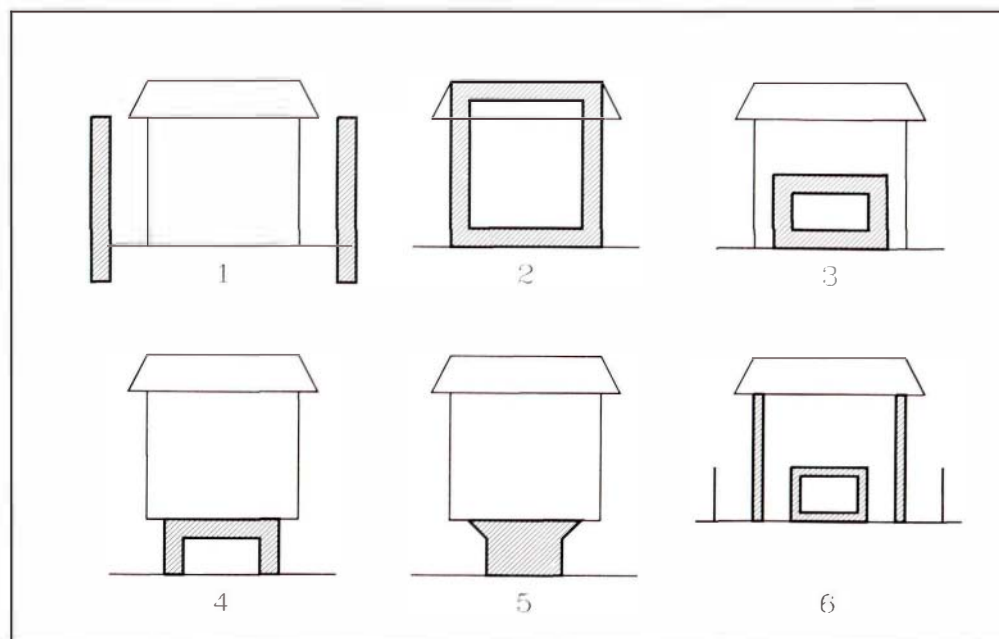
Twijnstra en Gudde NV heeft in 1986 een onderzoek gedaan naar de integrale werkplekkosten in kantoorgebouwen voor financiële instellingen. Volgens de onderzoekers mag worden aangenomen dat de uitkomsten niet veel zullen verschillen van de werkplekkosten in andere situaties. Het resultaat van het onderzoek is in hier weergegeven. Uitgegaan is van circa 20 m²

De integrale jaarkosten van een werkplek

	Minimaal	Maximaal	Gemiddeld	Aandeel in % van het gemiddelde
1 Vaste kosten				
– totaal	2.000	5.000	3.500	23,0
2 Instandhoudingskosten				
– onderhoud	350	800	500	4,5
3 Gebruikskosten				
– schoonmaakkosten	300	400	350	2,5
– energiekosten	300	900	350	3,0
– bewakings- en receptiekosten	750	1.100	900	6,0
– cateringskosten	1.300	2.150	1.500	10,5
– beheerskosten	1.800	3.500	2.500	16,0
– kosten repro en interne post	800	3.000	1.750	11,0
– kantoorbehoeften	500	1.250	800	5,0
– inrichtingskosten	300	1.000	600	4,0
– telecommunicatiekosten	300	1.000	600	4,0
– datacommunicatievoorzieningen	1.000	2.500	1.750	11,5
Totaal			15.300	100,0

Bron: Jan Regterschot: Facility management, 1988/112

Er kunnen verschillende wegen worden bewandeld bij inbraakbeveiliging



bruto-vloeroppervlakte per medewerker. In de tabel is te zien dat bewaking en receptiekosten (= een onderdeel van beveiliging) zich een stevige middenmootpositie hebben verworven. De kosten daarvan bedragen bijvoorbeeld het dubbele van de kosten van 'energie'.

Naar aanleiding van deze gegevens merkt de auteur op dat "de vraag kan worden gesteld of de aandacht van de facilitaire organisaties in het verleden wel is uitgegaan naar de juiste onderwerpen. Zo is er de laatste jaren op allerlei fronten veel gedaan aan de beheersing van energie- en onderhoudskosten. (...) Er kan niet worden beweerd dat deze posten in hun geheel niet interessant zijn, maar hun aandeel in de totale integrale kosten is betrekkelijk gering met circa 3 à 3,5 procent."

De aanwijzing die de 'facility manager' hier krijgt, lijkt ons ook zeker relevant voor de ontwerper:

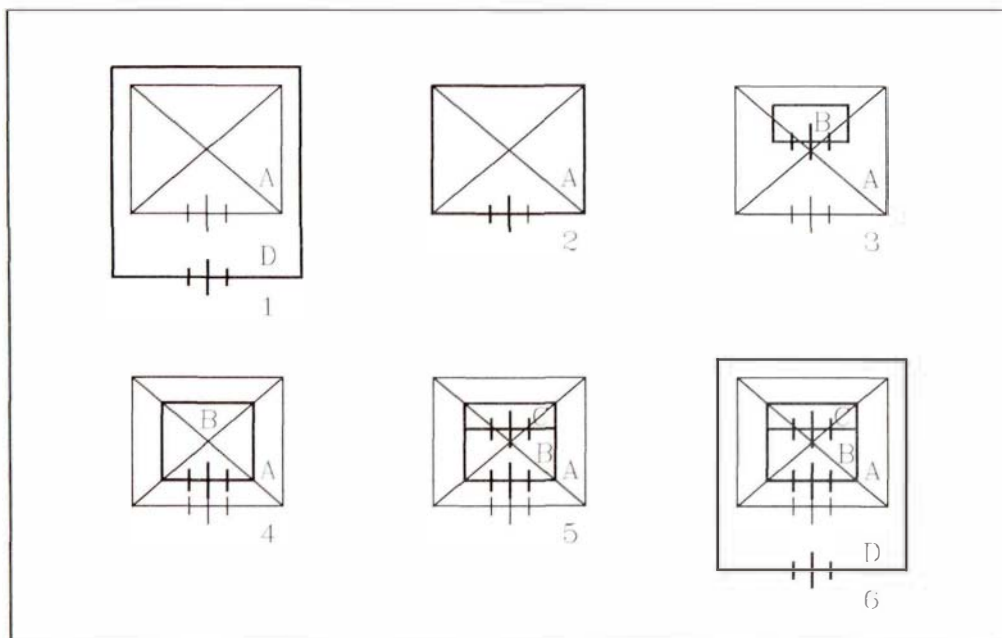
- Ten eerste omdat bewaking/toegangsbeheer een belangrijk onderwerp geworden is waar in het ontwerp rekening mee moet worden gehouden.
- Ten tweede omdat met het inbouwen van fysieke beveiliging geld te besparen valt in de beheerfase. Een ontwerp waar beveiliging is ingebouwd levert zijn geld op in de exploitatierekening.

- Ten derde zal zo'n ontwerp met 'inbouwbeveiliging' bovendien esthetisch-architectonisch hoger scoren. Het achteraf aanbrengen van voorzieningen is immers in het algemeen lelijk.

Ontwerper en beheerder kunnen kortom niet meer om het onderwerp beveiliging heen. En dat is ook logisch. Ten gevolge van de sterke toename van de criminaliteit in de afgelopen jaren lijkt het er (helaas) op dat bij veel kantoorgebouwen beveiliging niet langer als 'luze' mag worden beschouwd.

Criminaliteit kost het individu en de gemeenschap steeds meer. Het betreft hier niet alleen hoge kosten in meetbare geldbedragen, maar ook emotionele 'kosten' als gevoelens van onveiligheid bij de gebruikers. Niet alleen op basis van het principe dat voorkomen beter is dan genezen, maar ook op grond van een kosten/batenvergelijking kan men stellen dat beveiliging steeds lonender wordt.

Toch past hier een waarschuwing: de criminaliteitsrisico's zijn niet overal even groot. Het lijkt een aannemelijke veronderstelling dat een kantoorgebouw in de binnenstad van Rotterdam andere risico's kent in vergelijking tot een zelfde kantoorgebouw in een dorp in Friesland. De beveiliging



Ook bij toegangscontrole kunnen heel wat wegen worden behandeld

liging moet afgestemd zijn op de risico's die verwacht kunnen worden.

De wens om meer aandacht te besteden aan de bouwtechnische beveiliging van kantoren tegen de risico's van criminaliteit brengt ons op de vraag *hoe* men moet beveiligen.

Inbraakbeveiliging

In bijgaande schetsjes zien we een zestal willekeurige wegen die voor het bouwtechnisch beveiligen tegen bijvoorbeeld inbraak bewandeld zouden kunnen worden.

1 Omheinen:

Rond het kantoorgebouw zou een afscherming kunnen worden opgetrokken, met daarin een sterke, afsluitbare in- en uitgang.

2 Sterke buitenschil:

Gevels, gevelopeningen, dak en souterrain kunnen rondom consequent als een sterke buitenschil worden uitgevoerd.

3 Compartimenteren:

We laten het gebouw voor wat het is, maar op die plaats(en) waar het nodig is, wordt een sterk compartiment aangebracht.

4 Gebouw op plint:

Wederom laten we het gebouw voor wat het is, maar we plaatsen het gebouw bij-

voorbeeld op een hoge 'plint'.

5 Gebouw op poot:

Een variant op de plint is het plaatsen op een hoge poot; een oplossing die in de praktijk wordt toegepast.

6 Een mix van oplossingen:

In de praktijk zal veelal worden gekozen voor een 'mix' van oplossingen; voldoende aandacht voor afscherming rondom het gebouw, gecombineerd met buitenconstructies van voldoende fysieke weerstand en compartimentering.

Toegangscontrole

We lopen even vooruit op de elders in dit rapport te noemen definities en nemen aan dat *toegangsbeveiliging* (of *toegangsbeheer*) valt onder te verdelen in *inbraakbeveiliging* en *toegangscontrole*.

Toegangscontrole richt zich vooral op de beveiliging tijdens werktijd, en inbraakbeveiliging op de beveiliging na sluitingstijd. Net als bij de hiervoor genoemde zes te bewandelen wegen voor inbraakbeveiliging, kunnen we ook een soortgelijk aantal wegen — maar wel geheel andere — voor toegangscontrole bewandelen.

1 Omheinen:

Rond het kantoorgebouw kan een hoog hekwerk opgetrokken worden met een

'portier bij de poort' die er op toeziet of iemand bevoegd is het terrein en dus ook het kantoor te betreden.

2 *Blinde buitengevel:*

De gevels op begane-grondniveau worden volledig blind uitgevoerd, met één toegang en een portier zoals hiervoor omschreven.

3 *Compartimenteren (1):*

Welaten het gebouw voor wat het is (iederen mag vrij in en uitlopen); alleen op die plaats(en) waar het nodig is zorgen we voor een blind compartiment, wederom met portier.

4 *Compartimenteren (2):*

Dezelfde situatie als in 3, maar nu met een 'vrij toegankelijke' (publieks)ruimte A, een consequent uitgevoerd compartiment B en een min of meer normale kantoorruimte C.

5 *Compartimenteren (3):*

Dezelfde situatie als in 4, maar in het compartiment nog eens een compartiment van nog 'hogere orde'.

6 *Een mix van oplossingen:*

Ook bij toegangsbeveiliging zal — net zoals bij inbraakbeveiliging — in de praktijk vaak voor een 'mix' van oplossingen worden gekozen, waarbij met de som van alle maatregelen het gestelde doel kan worden bereikt. Een planmatige aanpak en een vakkundige uitvoering zijn ook hier een voorwaarde.

Leeswijzer

Dit rapport richt zich in de eerste plaats op nieuwbouwsituaties; ideeën en technieken voor verbouwingen kunnen daaruit worden afgeleid.

De hoofdstukken 1 tot en met 6 vormen de beschouwelijke ondergrond voor de technische uitwerkingen die in de hoofdstukken 7 tot en met 11 worden gegeven.

Een beschouwing vooraf is van belang voor het onderwerp beveiliging. Te vaak wordt de beveiliging achteraf even vluchtig afgedaan met een stukje 'hi-tech'-elektronika, hetgeen vaak tot problemen leidt.

Hoofdstuk 7 draagt de mogelijkheden en referenties aan voor het bouwtechnisch beveiligen tegen de risico's van *inbraak*, waarbij frequent wordt verwezen naar eer-

dere SBR-publikaties in de serie Beveiliging van gebouwen.

Hoofdstuk 8 gaat in op de meest voorkomende *compartimenten* in kantoorgebouwen: computer-, archief- en kluisruimten, alsmede de vaak onmisbare brand- en inbraakwerende kasten. Er wordt voor wat betreft dit laatste vooral op de kwaliteit van deze produkten ingegaan, omdat de keuze groot is.

In de hoofdstukken 9 en 10 ligt het zwaartepunt van dit rapport: de *toegangsbeveiliging*. Een wijdverbreide misvatting is dat toegangsbeveiliging alleen maar 'een systeem met magneetkaarten en wat elektronika' is. Missers betreffen vaak bouwkundige details.

Voor kantoren die over een eigen terrein beschikken, wordt in hoofdstuk 11 ingegaan op de *terreinbeveiliging*.

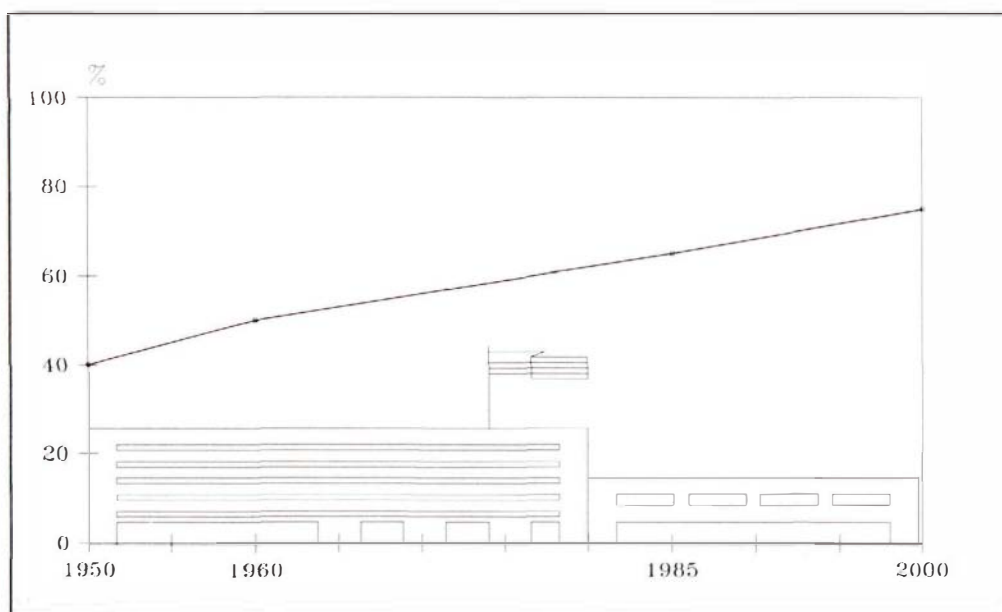
Ten slotte komen in hoofdstuk 12 de meest belangrijke aspecten van *vandalisme* aan de orde.

Het rapport wordt gecompleteerd met de inhoudsopgaven van eerder verschenen delen en het aankomende deel 5 in deze serie op beveiligingsgebied, een literatuur-opgave en de namen en adressen van relevante organisaties en instellingen.

Het woordenboek omschrijft een kantoor als een werkruimte, of een samenstel van werkruimtes voor administratieve werkzaamheden.

Deze omschrijving geeft alles behalve een compleet beeld van wat een kantoorgebouw is. Kantoren zijn in onze maatschappij steeds belangrijker geworden en die ontwikkeling lijkt niet te stuiten.

Er zijn verschillende soorten kantoorgebouwen. Om in de grote verscheidenheid enige ordening aan te brengen, zullen we op basis van een aantal primaire en secundaire kenmerken enig onderscheid maken.



Aandeel kantoorwerk ten opzichte van andere soorten werk in %

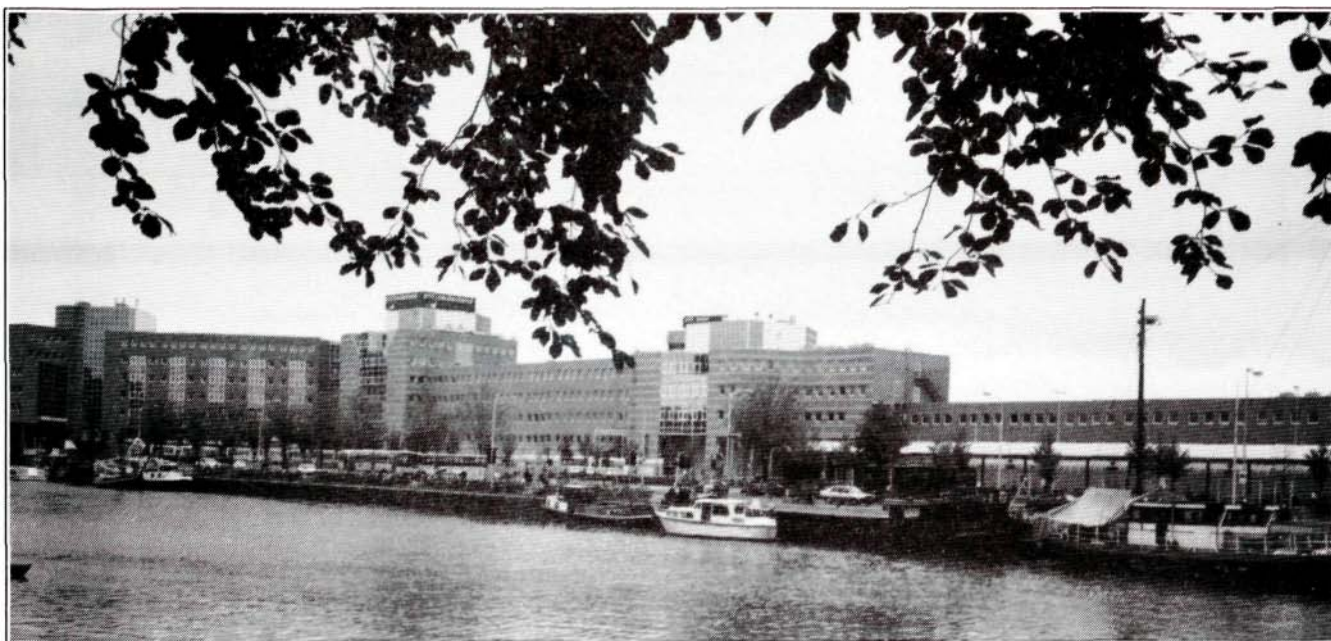
Grootte

Er zijn grote en kleine kantoren. Enerzijds omdat er grote en kleine bedrijven zijn, anderzijds omdat het ene bedrijf meer administratieve ondersteuning behoeft dan het andere. De grootte van het gebouw zou (zeker in combinatie met het type gebouw) een relatie kunnen hebben met criminele risico's. Zo bleek uit Engels onderzoek (Hope, 1982) dat voor wat betreft scholen (!) grote, lage en op het maaiveld uitgedijde scholen relatief meer last hadden van vandalisme en inbraak. Op zich is dit niet verwonderlijk: zo'n gebouw heeft meer (en eenvoudiger bereikbare) muren, deuren en ramen die vernield en/of opgebroken kunnen worden. Iets dergelijks zou ook voor kantoorgebouwen kunnen gelden.

Locatie

Hoewel de criteria voor de locatiekeuze in de loop der jaren nogal eens zijn veranderd, wordt de keuze vaak bepaald door de bereikbaarheid. Dat heeft voor de ligging van een kantoor nogal wat consequenties. Om een goede bereikbaarheid voor auto's te waarborgen zijn er de laatste jaren veel kantoorgebouwen aan uitvalswegen gebouwd. Daarnaast zijn ook intoenemende mate terreinen in de directe nabijheid van NS-stations geëxploiteerd.

Het spreekt voor zichzelf dat de locatie een vrij directe relatie heeft met de criminele risico's die een kantoor te duchten heeft. Het maakt een verschil of het kantoor op een stil en enigszins afgelegen bedrijfsterrein ligt, of midden in een stads-



*Uitgedijd kantoorgebouw
(gelegen nabij een
NS-station)*

centrum aan een drukke verkeersroute. Helaas bestaan geen onderzoeksgegevens over de spreiding van risico's voor bedrijfsgebouwen en kantoren. Kijkend naar andere gebouwtypen is te vermoeden dat het afgelegen bedrijfsterrein minder risico loopt, zeker waar het vandalisme betreft; de daders komen daar gewoon niet. Anderzijds zou men echter de hypothesen kunnen volgen dat afgelegen gebou-

wen *als* ze 'gepakt' worden, veel zwaarder 'gepakt' worden. De daders worden immers niet gestoord.

Publiek

Bij elk kantoor is over het algemeen sprake van bezoekend publiek. Als er van een grotere aanloop sprake is, zullen speciale ruimten moeten worden gemaakt voor de

*Traditioneel
notariskantoor*



ontvangst van het publiek. De scheiding van deze bezoekersruimten van de werkruimten vraagt veel aandacht, omdat bezoekers en kantoorbewoners elkaar toch zullen moeten ontmoeten.

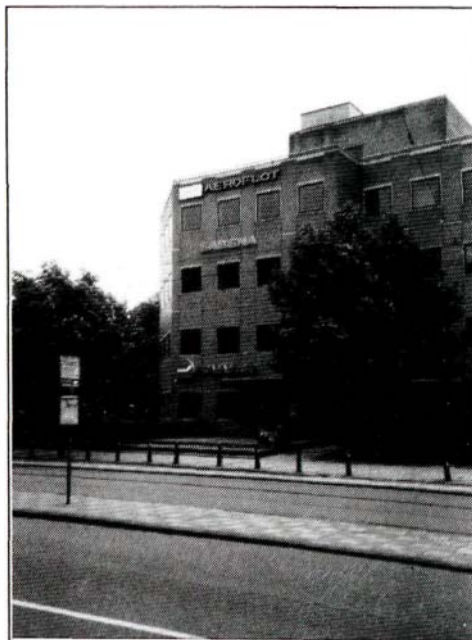
Vanuit beveiligingsoogpunt bezien vormen deze 'mensenstromen' eigenlijk de essentie van de beveiligingsproblematiek bij kantoren.

Ondersteuning

Vaak zal een kantoor ondersteuning bieden aan een bedrijf. We wijzen er met nadruk op dat we ons in dit deel beperken tot het kantoorgebouw zelf. In het vijfde deel van de reeks Beveiliging van gebouwen komen de bedrijfsgebouwen aan de orde waarbij een eventueel kantoor slechts één van de onderdelen van het geheel is (naast magazijn, productie/opslaghallen, terrein en dergelijke).

Specifiek

Kantoren worden soms voor een vaste functie of een vaste gebruiker gebouwd. Veel kantoorruimte wordt echter gebouwd voor een nog nader te bepalen gebruiker en voor een nog nader te bepalen gebruik. Zo groeide in de periode



Eén kantoorgebouw, meerdere huurders

1970 tot nu het aandeel gehuurde gebouwen van enige procenten tot circa 35% voor de kantoorsector en circa 25% voor bedrijfsgebouwen (Bleker, 1988/58).

Het zal duidelijk zijn, dat huur en koop elk hun eigen eisen stellen. In het ene geval is er sprake van een duidelijk omlijnd programma, waarbij ook beveiligingstechnisch al een nadere detaillering mogelijk is. In het andere geval is de grootst moge-



Kantoorgebouw voor meerdere gebruikers met gescheiden entree's

lijke flexibiliteit vereist ook voor wat betreft de beveiliging. Zolang men niet weet wie of wat in het gebouw komt, is elke vorm van beveiliging boven het standaardniveau misschien weggegooid geld. Juist in zo'n geval is het echter essentieel om ook voor eventueel veel zwaardere beveiligingsmaatregelen de opties open te houden!

TRENDS, PRIJS EN AFNEMERS

Aanbod-trend

Sinds 1979 presenteert het blad Vast-GoedMarkt (VGM) jaarlijks de resultaten van een enquête naar het gereed en in aanbouw zijnde aanbod van commercieel onroerend goed (gesplitst naar kantoren, bedrijfsruimten en winkels/showrooms), voorzover zij aan de bepaalde minimale oppervlakte-criteria voldoen.

Specifiek voor kantoorruimte ziet het aanbodbeeld er als in onderstaand overzicht uit.

Men ziet dat per ultimo 1988 1.673.000 m² kantoorruimte vrij voor de markt gereed of in aanbouw was. Het aanbod van kantoorruimten is voor ongeveer 80% in de Randstad geconcentreerd. Dit is een ge-

geven dat sinds 1979 (het begin van de VGM-enquête) onveranderd blijkt.

Naar aanleiding van hun enquête doen de auteurs met betrekking tot kantoorruimten enkele aanbodvoorspellingen die zeker ook hier interessant zijn:

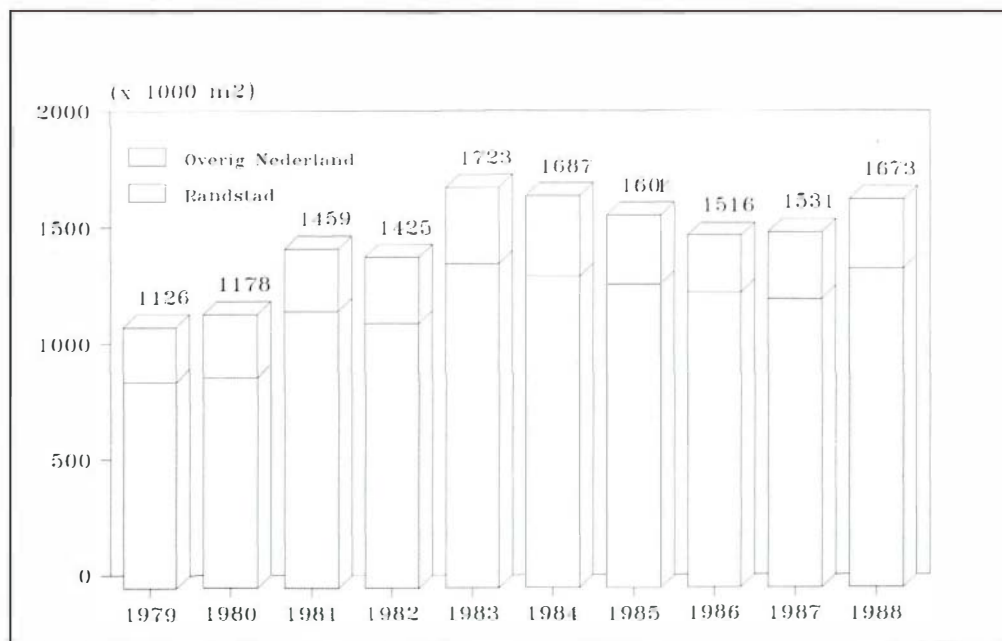
Er wacht méér aanbod op de kantorenmarkt zowel via reeds nu bestaande gebouwen als via het indrukwekkende stuwmeer aan ontwikkelingsprojecten.

"(...) Macro gezien zou (...) kunnen worden gesteld dat toekomstige gebruikers sowieso hun keuze kunnen doen uit 1,67 mln m² nu aangeboden ruimten, "enkele honderduizenden" m²'s die in de komende jaren als gevolg van nu reeds bekende verhuizingen vrijkomen, alsmede uit de bijna 4 mln m² die nog in voorbereiding zijn. *Ofwel globaal gezien staan tegenover elke reeds bestaande, beschikbaar zijnde of komende m², er bijna twee die nog op de tekentafel staan.*" (Rompelman en Van Deelen, 1989/5-7)

Opname-trend

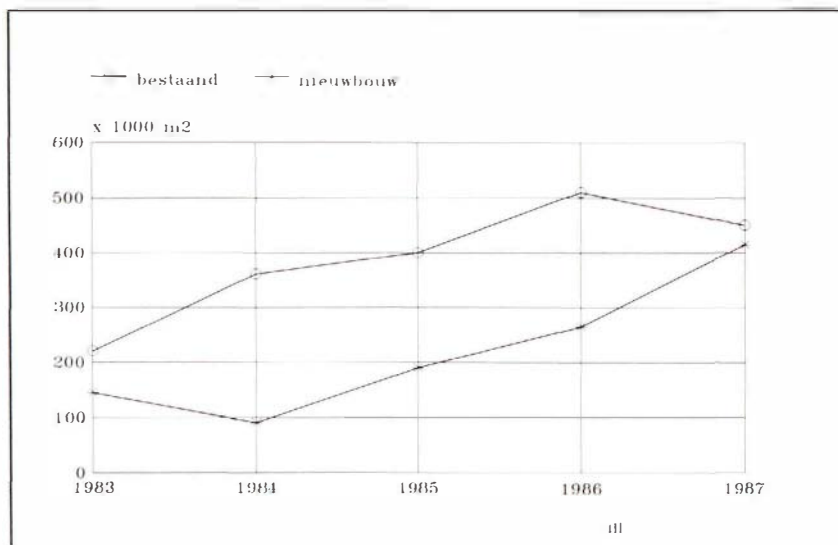
Het aanbod geeft een beeld van één kant van de medaille. Daarnaast moet natuurlijk ook gekeken worden naar de opname- (of transactie-) kant. Meer informatie hierover geeft een publikatie van Zadel-

Aanbod kantoorruimte in Nederland 1979-1988 (per ultimo)



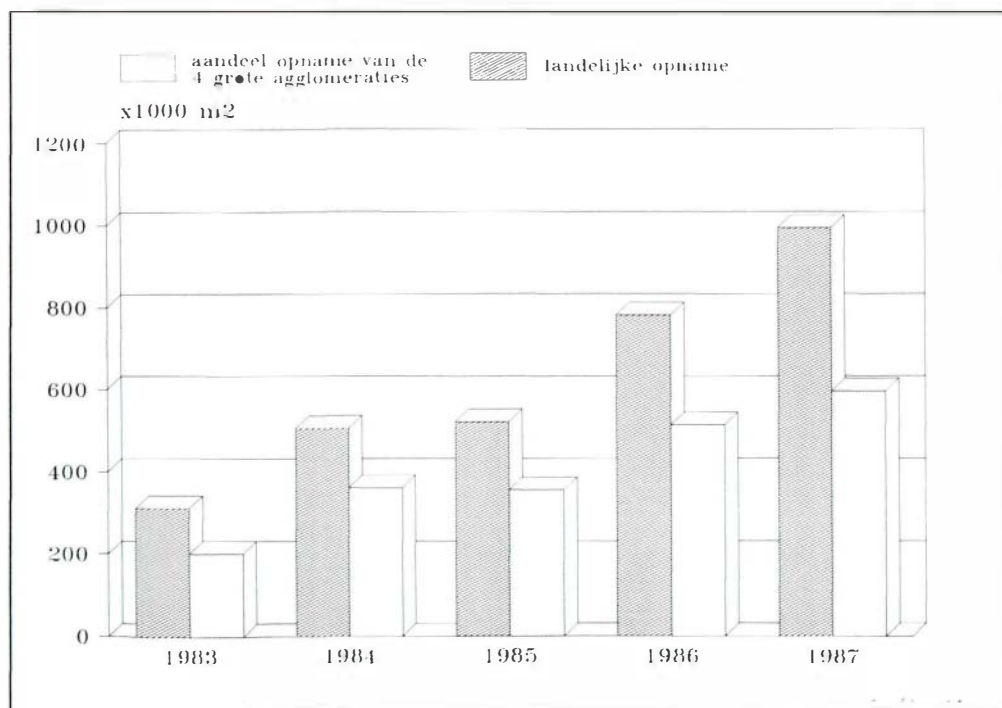
hoff/Universiteit van Utrecht uit 1988. Daaruit blijkt dat de opname op de 'vrije' kantorenmarkt (gemeten in transacties vanaf 500 m²) de afgelopen jaren enorm is toegenomen. De groei hangt nauw samen met het economisch herstel in Nederland. Een herstel dat eerder inzette dan de figuur aangeeft. De kantorenmarkt heeft kennelijk met een naijlingscfect van circa twee jaar gecageerd.

"Daarnaast heeft ook de indexering van de huren in bestaande kantoren haar invloed uitgeoefend. Mede als gevolg van relatief gedaalde bouwkosten (sterk toegenomen concurrentie) konden elders nieuwe kantoren worden aangeboden, vaak op goede lokaties, tegen huisvestingslasten die lager uitkwamen dan die in de achter te laten (verouderde) ruimte. De verschuiving in prijs/kwaliteitsverhoudingen, waardoor ook de servicekosten in het algemeen omlaag gingen, en 'weglok'- en 'uitkoop'-activiteiten van verhuurders van nieuwbouwkantoren (zoals bijdragen in de verhuis- en inrichtingskosten, huurvrije perioden en dergelijke) stimuleerden de nieuwbouw." (Zadelhoff, 1988/6) Het effect van een en ander wordt duidelijk aangetoond in de figuur (boven).



"De groei is echter ook een gevolg van de zich wijzigende eisen bij veel kantoorgebruikers. Men wenst een efficiënt en herkenbaar kantoor te betrekken waarbij niet alleen organisatorische, maar vooral juist ook technologische ontwikkelingen eisen aan de nieuwe huisvesting stellen. De afgelopen vijf jaar heeft ook een opvallende verschuiving te zien gegeven in de vraag naar architectonische kwaliteit. Vooral de ontwikkelingen op het gebied

Gemiddelde jaarlijkse opname commerciële kantorenmarkt in de periode 1983-1987



Totale opname op de vrije kantorenmarkt 1983-1987 (in gebouwen waarin 500 m² of meer te aanvaarden is)

in Noord-Amerika hebben hiervoor, uiteraard op Nederlandse schaal, model gestaan. Prestige-overwegingen zijn van groter belang geworden." (Zadelhoff, 1988/7)

Prijs

Op de kantorenmarkt zijn de regionale prijsverschillen vrij gering. De verschillen zijn in hoofdzaak afhankelijk van de geleverde kwaliteit (Zadelhoff, 1988/24 e.v.).

Afneemers naar type gebruikers

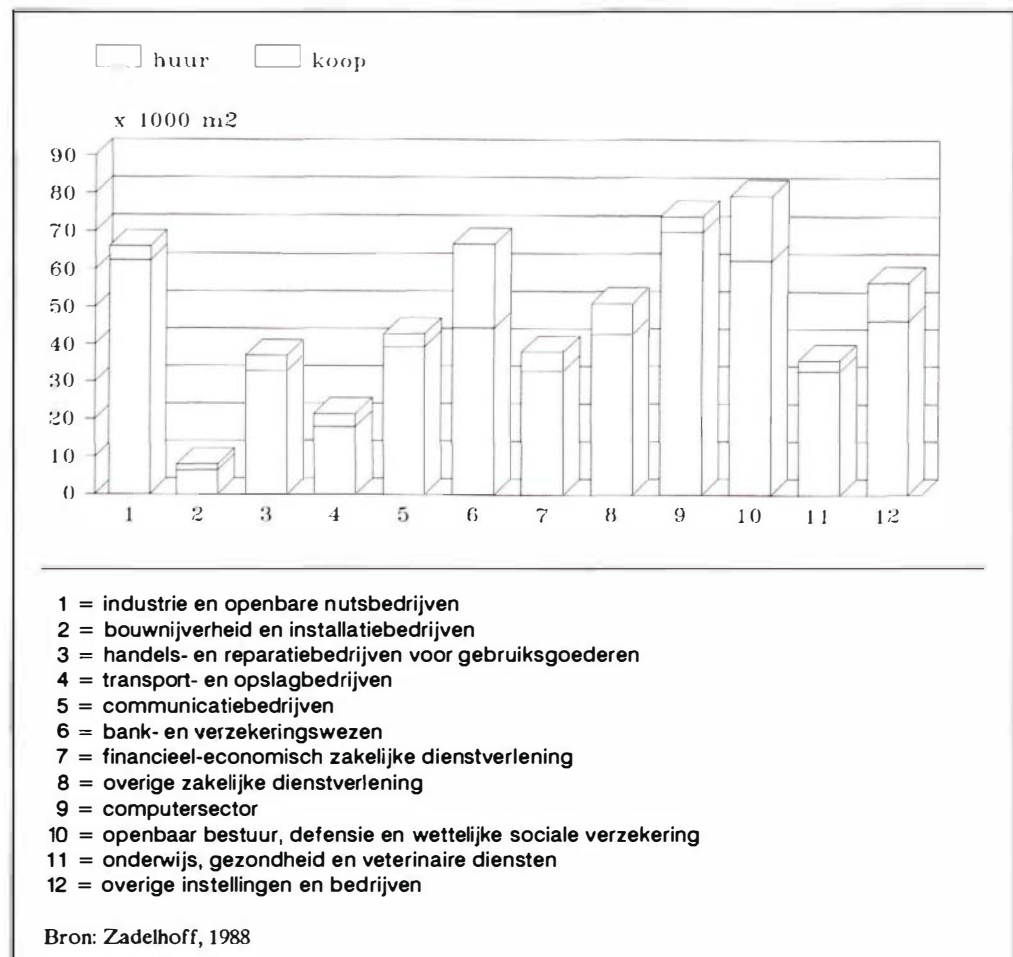
De (semi-)overheid in al haar geledingen is een belangrijke afneemster op de kantorenmarkt. Wanneer het hele (semi-)overheidscomplex als een groep zou worden gezien, dan blijkt dat de overheid in de periode 1983 tot en met 1987 rond

850.000 m² kantoorruimte (gemiddeld 170.000 m² per jaar) op de vrije markt heeft gehuurd dan wel gekocht. Dat is bijna 27% van de totale opname.

Ondanks deze stevige positie van de (semi)overheid als afneemster op de kantorenmarkt, blijkt dat toch ongeveer driekwart van de opgenomen kantoorruimte door het bedrijfsleven gehuurd/gekocht werd. Vanuit het bedrijfsleven zijn de computersector (met gemiddeld 75.000 m² per jaar) en het bank- en verzekeringswezen (met gemiddeld 70.000 m² per jaar) de belangrijkste afneemers.

Om meer inzicht te krijgen in de verschillende categorieën is in de volgende figuur een onderverdeling gemaakt naar de meest voorkomende hoofdgroepen, te weten bijna 85% van het totale transactievolume.

Gemiddelde commerciële kantooropname per jaar, per gebruiker, in de periode 1983-1987



Voordat er verder kan worden gesproken over de beveiliging van gebouwen, zullen we een idee moeten hebben waartegen er beveiligd zal moeten worden. Pas als duidelijk is wat er gebeurt of kan gebeuren, hoe de te verwachten ontwikkeling is en wat de omvang van de risico's is, kan een goed plan worden gemaakt voor de nabije en wat verdere toekomst. *Beveiligen zonder kennis te hebben van de risico's (qua aard, omvang en ontwikkeling) is per definitie geld weggooien*; men beveiligt dan immers te zwaar en/of te veel (zonde van het geld), te licht en/of te weinig (vals gevoel van veiligheid), of men beveiligt zich tegen de verkeerde dingen.

Aangezien over de criminaliteitsrisico's die het bedrijfsleven loopt nauwelijks iets bekend is en we er vanuit mogen gaan dat het bedrijfsleven het leeuwendeel van de in Nederland bestaande kantoorgebouwen bevolkt (zie hoofdstuk 2), valt er weinig te zeggen over de criminaliteitsrisico's van kantoorgebouwen.

Algemene risicogegevens ontbreken overigens niet alleen in Nederland maar ook in Engeland en de USA.

Het is dan ook niet verwonderlijk dat twee Amerikaanse onderzoekers de volgende conclusie trekken naar aanleiding van een zeer uitgebreide evaluatie van het effect van de bouwtechnische beveiliging van bedrijfsvestigingen:

“Men is geneigd aan te nemen dat een beveiligingsexpert de potentiële criminaliteitsproblemen vaststelt voor een bedrijfsvestiging, voordat hij zijn beveiligingsaanbevelingen doet. We constateerden echter bij herhaling dat er aanbevelingen gedaan werden, onafhankelijk van de *mogelijke* criminaliteitsproblemen. Sterker nog: de bestaande beveiligingscontrolelijsten bevatten eenvoudigweg niets waarmee rationele (dat wil zeggen doelgerichte en consistente) beveiligingsaanbevelingen ontwikkeld kunnen worden; ze sommen simpelweg alle mogelijke aanbevelingen op.

Samenvattend pleiten we dan ook voor de ontwikkeling van een *beveiligingscontrolelijst* waarmee *wel* rationele aanbevelingen gedaan kunnen worden. Zo'n controlelijst zou expliciet in moeten gaan op het 'risico' dat een bedrijfsvestiging loopt voor wat betreft bijvoorbeeld inbraak. De contro-

lelijst* zou een 'inbraakrisico-berekeningsmodel' moeten bevatten.”(Tien en Cahn, 1986/246)

Voor het bedrijfsleven (laat staan voor kantoorgebouwen) valt zo'n risicoberekening eenvoudigweg niet te maken, omdat de basisgegevens ervoor (politiecijfers, slachtofferonderzoeken) ontbreken.

Over vragen als:

- welk type criminaliteit;
- in welke omvang (aantal/schade);
- waar;
- wanneer;
- enz.

tasten we dus met betrekking tot het bedrijfsleven grotendeels in het duister.

De vraag rijst hoe het dan zit met '(rationaal) risk management'. Het bedrijfsleven doet toch juist heel veel aan het inschatten van de criminaliteitsrisico's en de preventie van die risico's?

De waarheid is anders. Weliswaar wordt er heel veel gepraat over 'risk management' maar daarvan hoeft men niet echt onder de indruk te zijn: het betreft hier vaak de verkoop van gebakken lucht. In essentie gaat het bij risk management om de vraag hoe het bedrijf zo goedkoop mogelijk beschermd kan worden tegen risico's (in ons geval: criminaliteitsrisico's).

Voor de risk manager staan dan vier wegen open (we citeren hier de VNO-handleiding beveiliging pagina 69/70):

- “het risico met open ogen accepteren en niets doen;
- geen preventieve maatregelen nemen, doch het risico verzekeren;

* = Tien en Cahn spreken hier over een 'security survey instrument'. Met andere woorden een beveiligingsonderzoeksinstrument: een beveiligingscontrolelijst voorafgegaan door een risicoberekeningsmodel.

- preventieve maatregelen nemen en niet verzekeren;
- zowel preventieve maatregelen nemen als verzekeren.”

De VNO-handleiding vervolgt dan:

“Bij het afwegingsproces voor het nemen van beleidsbeslissingen terzake komen aan de orde:

- de soort van mogelijke beveiligingsmaatregelen;
- een kosten/baten-analyse.

Bij dit alles mag niet uit het oog verloren worden, dat geen twee ondernemingen dezelfde zijn. Zij verschillen elk van aard, personeel, ligging, grootte, inrichting van gebouw, voorhanden materialen en de belangen die moeten worden beschermd.

Daardoor zal de inventarisatie van de mogelijke risico's en de te nemen beslissingen, zoals hiervoor beschreven, voor elk bedrijf een andere uitkomst geven.”

En met die laatste zin is de risk manager terug bij de opgave: de mogelijke risico's moeten eerst geanalyseerd worden.

Via de wet van de grote getallen kunnen grote bedrijven met veel vestigingen misschien nog wel een redelijk beeld krijgen van de relevante factoren die een samenhang vertonen met de ondervonden risico's. Op grond daarvan kan een beveiligingsbeleid (risk management) worden gevoerd.

Alle andere bedrijven (kleinere en/of met minder vestigingen) kunnen zich echter alleen maar baseren op hun zeer beperkte ervaring. Ze hollen daarmee per definitie achter de feiten aan. Het alternatief om de risico's voor te blijven is om dan maar van alles zo veel mogelijk te doen (je weet maar nooit wat er *kan* gebeuren).

Het dilemma is daarmee volstrekt helder: of je beveiligt te laat, of je beveiligt te veel en/of te zwaar.

Zolang er geen betere onderzoeksgegevens over criminele risico's voorhanden zijn, valt hier helaas weinig aan te doen. Toch willen we in de volgende paragrafen het weinige materiaal presenteren dat er bestaat over de criminaliteitsrisico's waar bedrijfsgebouwen mee te maken hebben.

RISICO'S KANTOORGEBOUWEN

Algemeen

Over de criminaliteitsrisico's van kantoorgebouwen is weinig bekend. De reden daarvoor is dat kantoorgebouwen een zeer verscheiden categorie vormen. Er zijn overheidskantoren en niet-overheidskantoren; elke branche van het bedrijfsleven heeft kantoren, openbare en niet-openbare kantoren en dergelijke.

Het is niet aannemelijk om te veronderstellen dat criminaliteitsgegevens (politiecijfers, slachtoffergegevens) ooit standaard voor heel Nederland uitgesplitst zullen worden naar (kantoor)gebouwentypen.

Hieruit mag men overigens niet afleiden dat aan kantoren uit criminaliteitspreventief oogpunt geen aandacht hoeft te worden geschonken. Eerder is het tegendeel het geval: de schade ten gevolge van een inbraak, brandstichting of vandalisme kan enorm zijn. *Te weinig beseft men nog dat door op zichzelf geringe criminaliteitsrisico's soms een heel bedrijf stil kan komen te liggen.*

Welke delicten / welke schade

Recentelijk zijn er enkele studies verschenen waarin getracht wordt de omvang en de schade van criminaliteit voor de hele Nederlandse samenleving te berekenen (Van Dijk en Röell, 1988/ SMP, 1988). De verschillende schattingen variëren globaal tussen de 20 en 30 miljard gulden per jaar. Ongeveer de helft daarvan moet gezocht worden in de sfeer van de (fiscale) fraude en het misbruik van subsidies en voorzieningen. Het spreekt vanzelf dat daarbij met name de overheid het slachtoffer is. Voor ons is dit deel van het verhaal hier echter minder interessant.

Bij dit soort macro-economische berekeningen probeert men de getallen toe te rekenen naar de verschillende maatschappelijke hoofdgedingen (huishoudens, bedrijfsleven, overheid).

We richten ons daarbij op het bedrijfsleven, er vanuit gaande dat daar de meeste

kantoren te vinden zijn. We komen tot het nevenstaande overzicht.

De grootste schadepost wordt in dit overzicht gevormd door *vandalisme*. In navolging van Van Dijk en Roëll (1988), is dit cijfer gebaseerd op gegevens over schade bij door justitie behandelde misdrijven.

De onderzoekers van het Nederlands Economisch Instituut die — zoals ze zelf ook zeggen 'met veel natte vingerwerk' — dit overzicht samenstelden hebben hier echter een rekenfoutje gemaakt (zie ook SEC, 1989/16).

De post 'vandalisme' schatten ze daarvoor waarschijnlijk (veel) te hoog in. Voor ons doel maakt dat hier echter niet zo vreselijk veel uit. Als we er vanuitgaan dat de inschatting in werkelijkheid de helft lager ligt (hetgeen een redelijk reële inschatting lijkt) dan zouden inbraak en vandalisme ongeveer even hoog scoren: elk 600 miljoen schade per jaar.

De schade als gevolg van *winkeldiefstal* is ontleend aan gegevens, die door vertegenwoordigers van de branche zelf naar buiten zijn gebracht, en die worden bevestigd door een enquête onder een steekproef van detailhandelsvestigingen (de NIPO-enquête; zie ook deel 3 van deze reeks Beveiliging van gebouwen, bijlage 6).

Ondanks alle bezwaren, die er zijn tegen het gebruik van verzekeringsgegevens, kon de schade als gevolg van *inbraak* bij bedrijven alleen aan deze bron worden ontleend.

Fraude, waarvan bedrijven het slachtoffer zijn, betreft bijvoorbeeld niet betaalde schulden als gevolg van BV-fraude, fraude met cheques en betaalkaarten, het illegaal kopiëren van software en frauduleuze claims bij verzekeringsbedrijven.

Gegevens over de buit bij grote *roofovervallen* worden verzameld door de Centrale Recherche Informatiedienst; de genoemde 33 miljoen gulden is aan die bron ontleend.

Een deel van de door bedrijven feitelijk geleden schade als gevolg van criminaliteit is in deze totaalraming nog niet verdisconteerd. Dat geldt bijvoorbeeld voor de indirecte kosten, zoals stagnering in

Soort criminaliteit	Bedrag in mln guldens*
Winkeldiefstal	700
Inbraak	600
Vandalisme	1.273
Buit roofovervallen	33
Fraude	500
Totaal	3.106

* = Uitgedrukt in guldens 1985/1986.

Bron: SMP/NEI, 1988

Schaderamingen voor bedrijfsleven als gevolg van criminaliteit (1985/1986)

het productieproces omdat het bedrijf slachtoffer wordt van een misdrijf, omzetverlies omdat cliënten worden afgeschrikt, omzetverlies omdat door vormen van criminaliteit de concurrentieverhoudingen op goederenmarkten en de arbeidsmarkt worden verstoord enz.

Voor beveiliging van kantoorgebouwen kunnen we slechts de gegevens over de delicten inbraak, vandalisme en roofovervallen gebruiken.*

Ook roofovervallen worden hier niet behandeld. Het betreft namelijk vooral overvallen op geldinstituten, waarde-transporten en supermarkten.

Zeer globaal blijkt het bedrijfsleven dus van twee grote criminaliteitsrisico's last te hebben:

- inbraak;
- vandalisme.

Bij vandalisme gaat het in concreto om vernielingen van bedrijfsbezit.

VANDALISME

In deel 1 en 2 van deze serie over beveiliging van gebouwen: Eengezins- en Meergezinswoningen is al uitgebreid ingegaan op de achtergrond van vandalisme en waar het voorkomt. Daarnaast gaan we in hoofdstuk 12 van dit vierde deel nog nader in op het onderwerp vandalisme. Over de omvang, aard, spreiding, achtergrond en

* = Winkeldiefstal hoort immers thuis in deel 3 over winkels en is derhalve daar ook in de vorm van een korte bijlage besproken. Fraude is een delict dat nauwelijks een relatie heeft met het ontwerpen of beheren van gebouwen.

ontwikkeling van het vandalisme van kantoorgebouwen valt weinig te zeggen. We vermoeden dat het een van de top-risico's is, qua schade en ook qua omvang (aantal gevallen). In hoofdstuk 12 is bijvoorbeeld te zien dat openbare gemeentelijke kantoren na scholen en het GEB (lantaarnpalen!) als derde risicogroep genoemd staat.

Vandalisme wordt vooral gepleegd door jongeren van acht tot achttien jaar en de motieven per leeftijdsgroep verschillen van verkenning tot onvrede en tot wraak. Er zijn zowel interne als externe drempels om vanden te weerhouden en er moet een gelegenheid of object zijn om vandalisme op uit te oefenen (afleiding van het object).

In deel 2 van de serie Beveiliging van gebouwen werden de volgende strategieën voor vandalismpreventie gegeven en uitgewerkt.

Toezicht:

- 1 Vergroting van de zichtbaarheid;
- 2 Vergroting van de overzichtelijkheid;
- 3 Verbetering van de surveillancemogelijkheden voor politie en andere bewakingsdiensten;
- 4 Intensivering van voorzieningen en activiteiten.

Betrokkenheid:

- 5 Vergroting van de territorialiteit;
- 6 Verduidelijking van de functie van openbare gebieden.

Afweer:

- 7 Objectverstevinging;
- 8 Vermindering van de toegankelijkheid;
- 9 Vergroting van het onderhoudsgemak.

Esthetica:

- 10 Aspectenverbetering.

Het risico van vernielingen hangt vaak af van externe factoren. Doorslaggevend is over het algemeen het aantal jongeren dat in de buurt van het desbetreffende kantoor woont, uitgaat, rondhangt of er langs komt.

De kans op vernielingen wordt vergroot wanneer de branche waarin het kantoor zijn geld verdient bij sommigen ter discussie staat.

Daarbij hoeft niet per sé een politieke achtergrond te spelen. Ook kunnen er persoonlijke redenen zijn, zoals het niet-ontvangen van een uitkering of de afwijzing van een verzoek om een woning. In alle gevallen moet de moeite worden genomen om de kans op schade zoveel mogelijk te beperken en indien éénmaal schade is aangericht, deze zo snel mogelijk weer te herstellen. Hiervoor kunnen zowel bouwkundige maatregelen worden genomen als bewaking door mens en/of systeem, afhankelijk van de te verwachten problemen.

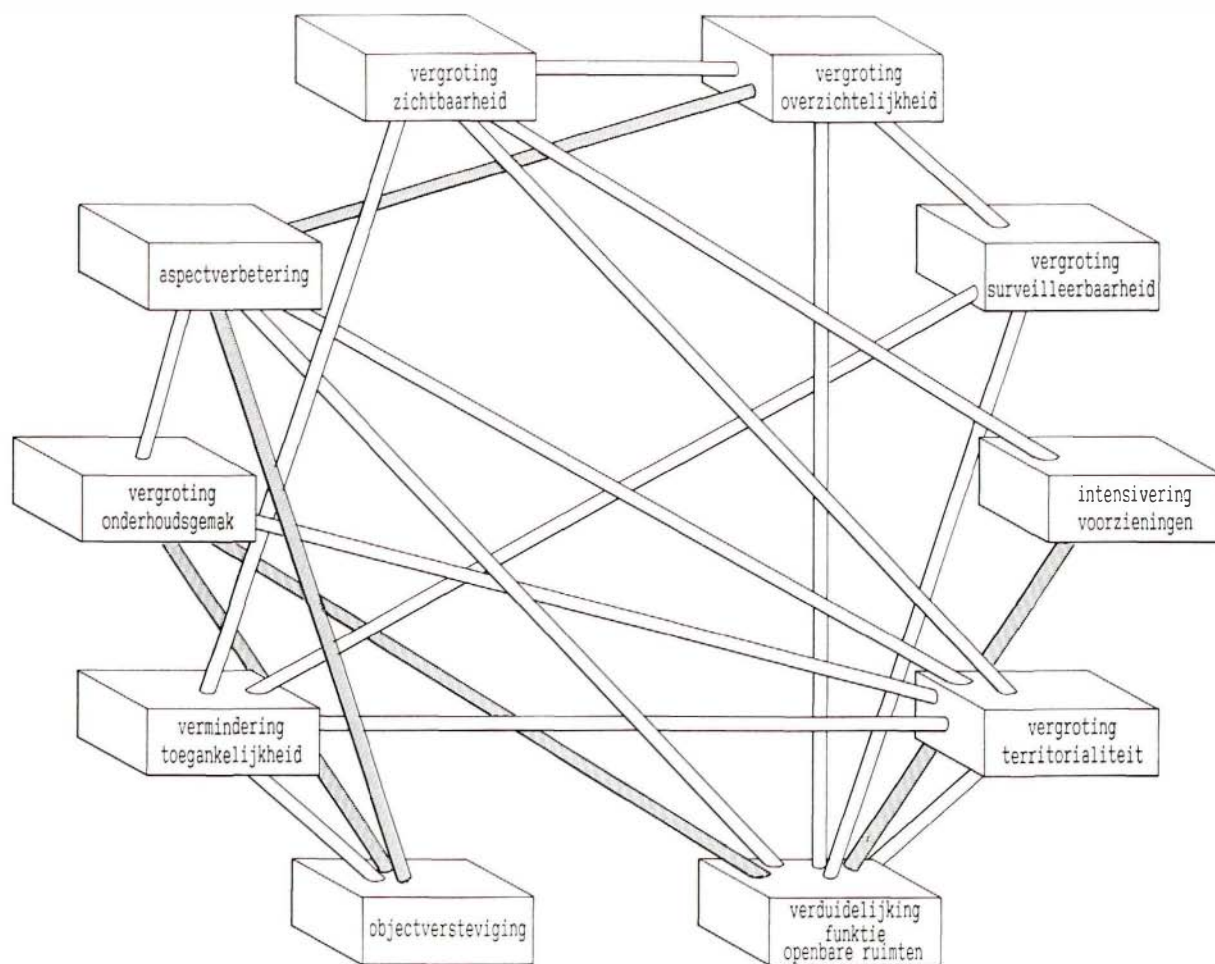
INBRAAK

De landelijke toename van het aantal inbraken geldt waarschijnlijk ook voor kantoorgebouwen. We kunnen dit vermoeden baseren op CBS-gegevens.

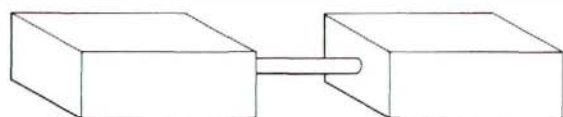
Sinds 1986 kent de CBS-politiestatistiek de categorie diefstal uit scholen/bedrijven. Onder diefstal wordt overigens ook inbraak verstaan. Winkeldiefstal valt er niet onder. Het betreft een zeer merkwaaardige en bovendien een uitermate onpraktische categorie. Niet alleen is het verband tussen scholen en bedrijven onduidelijk dan wel afwezig, maar ook het risico en de ontwikkelingen daarbinnen kunnen bij beide sterk verschillen.

Aangezien een inschatting niet mogelijk is, wordt er vanuit gegaan dat we met een gelijksoortige ontwikkeling te maken hebben. Aangezien er verhoudingsgewijs veel meer bedrijven zijn dan scholen (ongeveer 400.000 actieve bedrijfsvestigingen tegenover ruim 22.000 scholen), lijkt het aannemelijk dat de cijfers met name de criminaliteitsontwikkeling bij bedrijven weergeven. De tabel geeft een uitsplitsing naar regio (zie pag. 32).

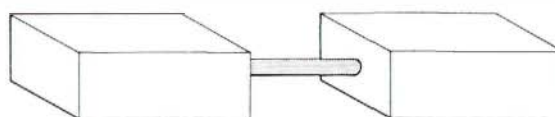
Bij deze tabel dient men te beseffen dat het hier (wederom) gaat om het bedrijfsleven als totaal. Gegevens specifiek over kantoren zijn niet beschikbaar. Tevens zij opgemerkt dat het in deze tabel het delict diefstal betreft. We vermoeden dat er in de meeste gevallen sprake zal zijn van een inbraak (of ten minste een insluiping).



STRATEGIEËN VOOR VANDALISMEPREVENTIE



strategieën versterken elkaar



strategieën werken elkaar tegen

Diefstal uit scholen/bedrijven exclusief winkeldiefstal (processen-verbaal (PV's) politie)

Regio	PV's 1986	%	PV's 1987	%	Index 1986	Index 1987
Friesland	1.702	2.6	1.746	2.4	100	103
Groningen	3.371	5.1	3.516	4.8	100	104
Drenthe	1.056	1.6	979	1.3	100	93
Overijssel West	1.529	2.3	1.741	2.4	100	114
Overijssel Oost	2.155	3.2	2.433	3.3	100	113
Gelderland Noord	1.905	2.9	2.218	3.0	100	116
Gelderland Midden	1.503	2.3	1.076	1.5	100	72
Gelderland Zuid	1.762	2.7	1.493	2.0	100	85
Utrecht	3.310	5.0	4.069	5.6	100	123
Noord-Holland N	2.047	3.1	1.867	2.5	100	91
Noord-Holland Z-W	1.700	2.6	2.445	3.4	100	144
Noord-Holland Z-O (incl. Amsterdam)	9.156	13.8	8.891	12.1	100	97
Zuid-Holland Mid.	3.964	6.0	5.451	7.4	100	138
Haaglanden	6.279	9.5	5.634	7.7	100	90
Rijnmond	5.833	8.8	8.377	11.4	100	144
Dordrecht	1.751	2.6	2.219	3.0	100	127
Zeeland	850	1.3	1.163	1.6	100	137
Noord-Brabant West	4.897	7.4	5.838	8.0	100	119
Noord-Brabant N	2.994	4.5	2.959	4.0	100	99
Noord-Brabant O	2.398	3.6	3.138	4.3	100	131
Limburg Noord	2.520	3.8	2.745	3.7	100	109
Limburg Zuid	2.196	3.3	2.178	3.0	100	99
Flevoland	1.533	2.3	1.064	1.5	100	69
Totaal	66.411		73.240		100	110
Bron: CBS						

We kunnen vaststellen dat in 1987 het aantal geregistreerde delicten met 10% is vermeerderd ten opzichte van 1986. Dit kan als een indicatie worden gezien dat er sprake is van een toename van het aantal diefstallen en inbraken in bedrijven. De tabel laat voorts zien dat de regio's die hoog scoren met name verstedelijkte gebieden betreffen. Dit laatste is op zich niet zo verwonderlijk aangezien in die regio's ook de meeste vestigingen staan.

Bij inbraken in kantoorgebouwen betreft het vermoedelijk enerzijds hetzelfde soort risico dat we bij de woningen al tegenkwamen (zie deel 1 en 2): de kleine dieven. Daarnaast zullen kantoren echter ongetwijfeld meer dan woonhuizen de dupe worden van professionele inbrekers.

Het samengaan van kantoorgebouwen en bijvoorbeeld bedrijfsgebouwen of geldkantoren kan hierbij leiden tot een verhoging van het risico, omdat daar vaak meer te halen valt dan in een puur administratief kantoor. De te nemen maatregelen ter voorkoming van inbraak richten zich voornamelijk op de tijd buiten de kantooruren en bestaan meestal uit het 'barricaderen' van een gebouw en zijn toegangen.

BRANDSTICHTING

Specifiek voor kantoorgebouwen bestaan wel gegevens over branden en brandschade. Het gaat hier niet om grote aantallen,

*Branden en brandschade
in kantoorgebouwen*

	Totaal aantal branden	Schade niet opgegeven	Zonder schade	Met schade	Met opgave schadebedr.	Schadebedrag (x 1.000 gld)
1985	152	5	43	104	83	10.788
1986	132	1	33	98	71	5.366
1987	131	—	25	106	81	11.727

maar de schade per geval is over het algemeen groot (gemiddeld meer dan een ton per geval).

Het is dus zeker interessant om te kijken hoeveel branden een criminele of baldadige achtergrond hebben. Daar blijkt in ongeveer een op de drie gevallen sprake van te zijn.

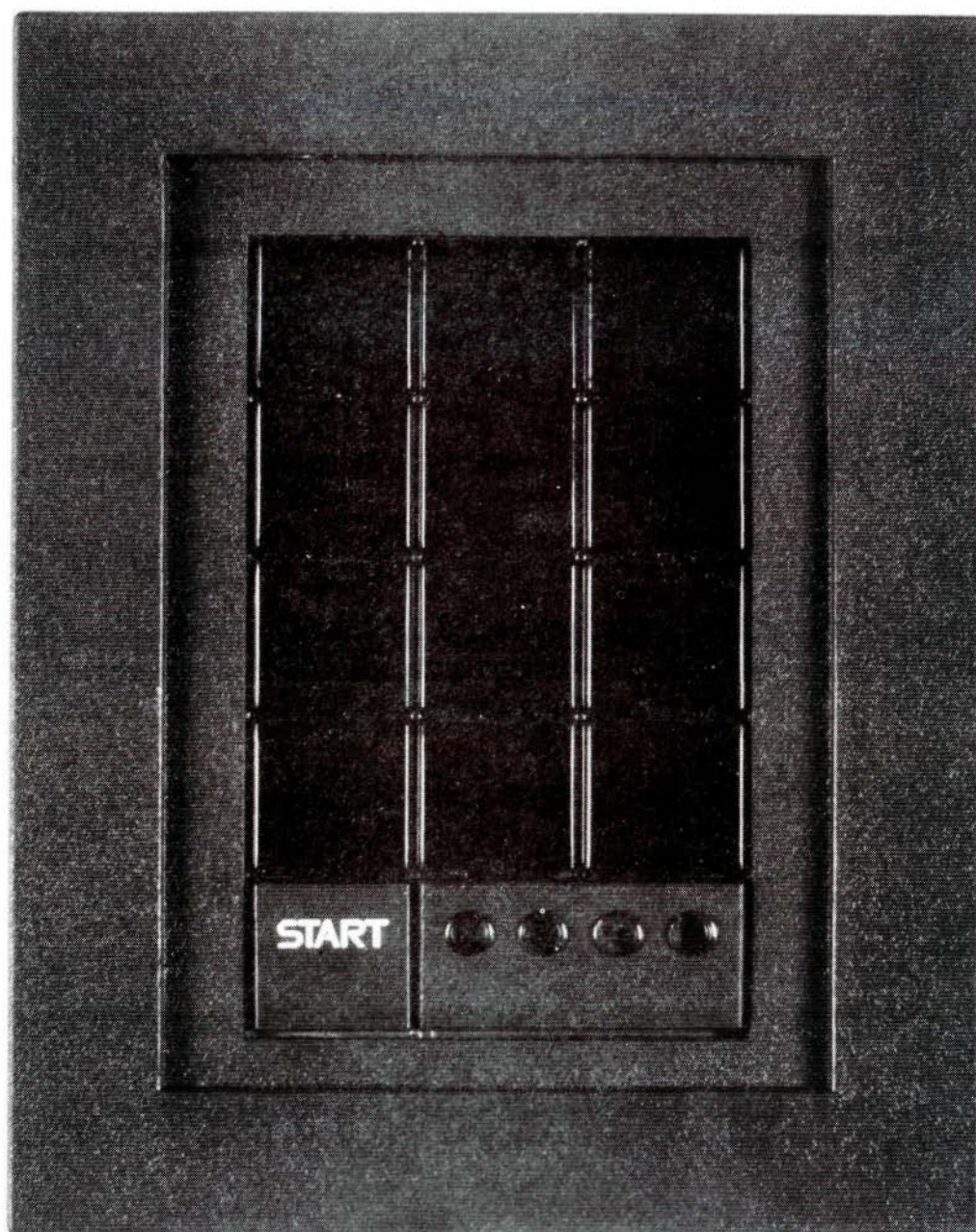
*Branden en brand-
oorzaken in
kantoorgebouwen*

Totaal aantal branden		Brandstichting		Spelen met vuur, baldadigheid		Overig*	
		absoluut	%	absoluut	%	absoluut	%
1985	152	37	24	8	5	107	71
1986	132	40	30	10	8	82	62
1987	131	28	21	5	4	98	74

* = De categorie overig omvat: onvoorzichtigheid bij roken; onvoorzichtige, ondeskundige behandeling; oververhitting/fel stoken; hitte-uitstraling; las- snij- en soldeerwerkzaamheden; defect/technische storing; vervuiling; afbranden van verf; bouw- en constructiefouten; lekkende gasleiding; sluiting; explosie; mechanische energie; statische elektriciteit/bliksem; zelfontbranding; chemische reactie;

OVERIGE RISICO'S

Het gaat in dit rapport om de meer algemene risico's die men loopt bij het gebruiken van een kantoorgebouw. Zelfs enige van de bovenstaande risico's, zoals brandstichting en gerichte vernieling, zijn al zoveel minder gebruikelijk, dat er verder relatief weinig aandacht aan zal worden besteed. We beperken ons dus tot de meest voorkomende risico's, maar tekenen daarbij aan dat diverse maatregelen ook voor zwaardere gevallen bruikbaar zijn.



Het is bij het nieuwbouw- en verbouwproces, een noodzaak, dat de opdrachtgever zijn wensen helder en duidelijk formuleert, zodat een architect weet wat er van hem verwacht wordt. Het is jammer dat dit weinig gebeurt. De opdrachtgever moet zijn wensen en eisen vastleggen op basis van een programma van eisen, met daarin aangegeven de benodigde ruimten, de grootte van de ruimten, de gewenste routing, afwerkingsniveaus, technische eisen, enz. Daarnaast zal er een richtprijs nodig zijn om de architect enige richting te geven. Op basis hiervan moet de architect aan het werk gaan en proberen in goede samenspraak met de opdrachtgever, een optimaal resultaat te behalen.

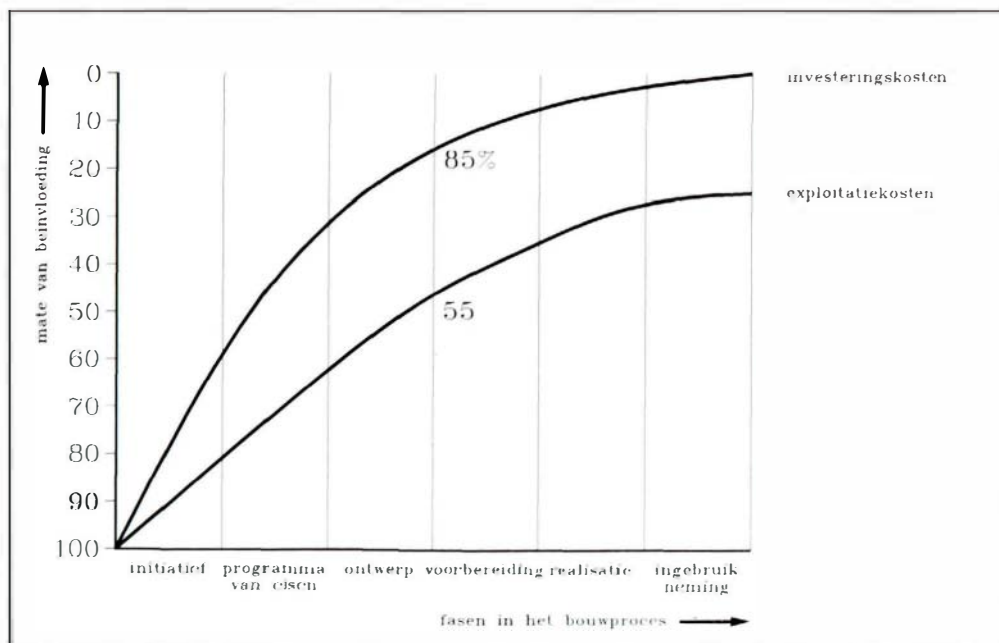
Daarbij zullen concessies nodig zijn op diverse gebieden, soms zelfs afgedwongen door derden, maar er zal een plan ontstaan waarin beide partijen zich moeten vinden. De architect heeft daarbij, dankzij zijn vaardigheden, de mogelijkheid om een opdrachtgever te wijzen op mogelijke verbeteringen in zijn programma om zo samen naar iets moois en bruikbaar te streven. Daarbij mag natuurlijk nooit worden vergeten, dat de opdrachtgever over een bepaalde periode gebruik zal maken van het gebouw, terwijl de architect dan al lang weer aan iets anders bezig is.

Daarbij dient men te beseffen dat een groot deel van de exploitatiekosten al in

het bouwproces zijn vastgelegd. Dat de investeringskostengedurende het verloop van het bouwproces snel aan beïnvloedbaarheid inboeten is alom bekend. Dat zo iets echter ook voor de exploitatiekosten opgaat beseft de ontwerper (en beheerder) vaak minder.

Uit de figuur blijkt dat met de keuze van het ontwerp 85% van de uiteindelijke investeringskosten zijn vastgelegd en daarmee 55% van de uiteindelijke exploitatiekosten van het gebouw.

Gezien het gewicht dat beveiliging in de schaal legt qua exploitatiekosten (zie ook hoofdstuk 1) verdient het dus alleen al uit het perspectief van het exploitatiemana-



De mogelijkheid om investeringskosten en exploitatiekosten te beïnvloeden gedurende het bouwproces

gement ten zeerste aanbeveling om in de initiatiefase, maar zeker bij het formuleren van het programma van eisen ruimte te reserveren voor het hoofdstuk 'beveiliging'. Het zal daarbij tevens duidelijk zijn, dat het invoeren van beveiligingsmaatregelen in tweede instantie, na de bouw, een veelvoud zal kosten van het meteen bij de bouw aanbrengen van dergelijke maatregelen. Zelfs bestaat de kans, dat zaken die in eerste instantie bouwkundig en zonder extra kosten kunnen worden opgelost, in tweede instantie niet meer kunnen worden opgelost of slechts op een slechte manier en tegen hoge kosten.

In het bestek-hoofdstuk 'beveiliging' zal een aantal risico-onderwerpen ter sprake moeten komen, een deel om te omschrijven waar het om gaat, een deel om de eisen te noemen die aan de uitvoering worden gesteld.

INVENTARISATIE EN DEFINITIE VAN DE RISICO'S

Allereerst moet worden aangegeven welke risico's men vreest. Gaat het om inbraak, vandalisme, overvallen, geweld gericht tegen werknemers of management. Of zijn het mogelijk acties van binnenuit? Hiermee zal een beeld gevormd kunnen worden of men zich moet beveiligen tegen voetgangers of tegen vrachtwagens, of men mensen van het gebouw weg wil houden of dat men slechts wil voorkomen, dat mensen binnenkomen.

DEFINITIE VAN GEBIEDEN

Het zal niet vaak gebeuren dat een heel gebouw moet voldoen aan dezelfde graad van beveiliging. Een computerruimte zal altijd beter beveiligd moeten zijn dan de kantine en in ruimten waar veel publiek komt, zullen andere maatregelen nodig zijn dan in de kamer van de directeur. Daarom moet bij de indeling van het gebouw zoveel mogelijk rekening gehouden worden met het bij elkaar situeren van ruimten met een zelfde veiligheidsbehoef-

te. Zo dienen ruimten met een publieksfunctie bij elkaar te komen, gebieden met waardepapieren of geld bij elkaar, enzovoort. Het mag daarbij niet zo zijn, dat de beveiligingsrangschikking voorrang krijgt boven de functionele rangschikking, maar vaak zal blijken dat die twee grote overeenkomst hebben. In elk geval zal blijken waar de frictie tussen beide zit en hiervoor zal een oplossing moeten worden gezocht. Bij verbouwing van ruimten of bij inpasning van een functie in een reeds bestaand kantoor, zal zelden sprake zijn van een ideale situatie. Er zullen meer technische dan bouwkundige oplossingen moeten worden gevonden. Maar ook bij nieuwbouw moet men zich afvragen of het mogelijk en zinnig is om maatregelen te voorzien die men niet meteen wil uitvoeren, maar wel uitvoerbaar wil houden. De kosten van de uitvoering in tweede instantie kunnen daarbij van doorslaggevende betekenis zijn. Bij de omschrijving van de te beveiligen gebieden moet men, naast de inpandige ruimten, niet vergeten om de buitenruimten te noemen en ook juist bij deze twee typen ruimten 'begint' de beveiliging van een gebouw. Het uiteindelijke doel van de definiëring zal een gewenste lay-out voor het gebouw zijn, waarin wordt aangegeven wie waar, wanneer en hoe wordt toegelaten. Een voor ontwerpers praktische werkwijze is op tekening per (groep van) ruimte(n) de te verwachten risico's aan te geven en dan (indien mogelijk) binnen het kader van het beveiligingsplan hiermee te gaan 'schuiven'.

DEFINITIE VAN BEVEILIGING

De volgende stap is de omschrijving van de manier waarop de gekozen gebieden worden beveiligd voor het omschreven risico. In het volgende hoofdstuk wordt als hulpmiddel bij deze stap een praktisch instrument (het Ruimte-risico-inschattingmodel: RRIM) gepresenteerd.

Het uitgangspunt van elke manier van beveiligen is: maak het de vandaal/inbreker zo moeilijk mogelijk, maar hinder de werknemers/klanten zo min mogelijk.

De mogelijkheden om hierin te voorzien, moeten in de eerste plaats van de bouwkundige maatregelen komen. In tweede instantie kan worden gekozen voor het tonen van pasjes of andere indentificatiemethoden en zo nodig kan bewakingspersoneel worden ingezet. De vele mogelijkheden voor toegangscontrole zullen verderop in dit rapport worden behandeld, evenals bouwkundige, inbraakpreventieve oplossingen.

BEZWAREN

Bij het opstellen van een beveiligingspakket, moeten steeds ook de bezwaren worden gezien. Het gaat niet alleen om een maximale beveiliging van gebouwen. Het eerste doel zal steeds blijven om een goed functionerend gebouw te maken. De bezwaren van een beveiligingspakket kunnen zowel van financiële aard als van personele aard zijn. Als een werknemer elke keer als hij naar het toilet gaat zijn pasje moet laten zien, zal hij geneigd zijn tot ontduiking of sabotage van het systeem. Onzes inziens zeer terecht in dergelijke hoge nood!

Bij het inpassen van een systeem zal men zich dus steeds moeten afvragen wat de kosten zijn, ook financieel, en wat de opbrengsten. Zo er toch bezwaren aan een oplossing blijven kleven, zal de moeite genomen moeten worden de mensen te overtuigen van het goede ervan en te blijven zinnen op verbeteringen.

GEBRUIKSVRIENDELIJKHEID

Bij het uitzoeken van oplossingen zal het gemak, waarmee een systeem kan worden gebruikt, van doorslaggevende betekenis moeten zijn. Daarbij zal gelet moeten worden op zowel de eenvoud van de handelingen die men moet verrichten, als de weerstand die mensen kunnen hebben om zich aan bepaalde maatregelen te moeten onderwerpen.

Stelregel bij de invoering van beveiligingen moet dus altijd zijn: zoek een systeem

dat begrijpelijk en overzichtelijk is voor iedereen. Elk systeem is te saboteren en wordt daardoor nutteloos, misschien wel extra hinderlijk. Hoe groter de hinder, hoe groter de inventiviteit voor ontduiking en sabotage.

CONTROLE EN ONDERHOUD

Na de keuze voor een manier of een systeem van beveiligen houdt het niet op. De keuze voor een leverancier of een fabrikant van een systeem is minstens zo belangrijk, want de meeste systemen, bouwkundig zowel als elektronisch, zijn waardevol als zij niet goed zijn gefabriceerd, uitgevoerd en/of geplaatst. Het zal dus zaak zijn om, na het juiste systeem, de juiste materialen/fabrikaten te kiezen, daarna de correcte installatie en de manier van inbedrijfstellen.

Het zal niemand verbazen, dat bedrijven die veel met bouw en met beveiliging te maken hebben, hiervoor specialisten in dienst hebben. Deze kennen de markt en weten welke eisen gesteld moeten worden aan de uitvoering.

Door 'beveiligingsleken' wordt soms wel degelijk de noodzaak van een in te winnen advies ingezien, maar daarbij wordt dikwijls een beroep gedaan op die mensen, die meer belang hechten aan de omzet dan aan een goed functionerend systeem. Om deze valkuil te ontlopen treft men dan ook in bijlage 2 een overzicht aan van de organisaties en instellingen zodat men zich allereerst op de markt kan oriënteren.

EN NU ... ?

In dit hoofdstuk is nog slechts in zeer algemene termen op het onderwerp 'beveiligingsplan' ingegaan.

De noodzaak van het maken en hebben van zo'n plan is aangegeven en er is in globale termen ingegaan op het *essentiële* punt dat beveiliging (en dus *elke* beveiligingstechniek) tenslotte gebaseerd is op een menselijk draagvlak.

Het is dan ook een keiharde randvoorwaarde dat beveiligingsmaatregelen in kantoren niet haaks mogen staan op de dagelijkse menselijke routine in kantoren.

Hierna volgt de vraag hoe men nu tot een concreet beveiligingsplan (als hoofdstuk op te nemen in het programma van eisen) kan komen. Het begin van dit hoofdstuk biedt daarvoor het aangrijpingspunt; we zagen immers dat:

- De basis van zo'n plan wordt gevormd door een 'berekening' of inschatting van de criminaliteitsrisico's.
- Het verdient aanbeveling om de verschillende ruimtes (of elementen) van het kantoorgebouw als uitgangspunt te nemen.

Met deze twee ingrediënten kunnen we in het volgende hoofdstuk concreet aan de slag.

RUIMTE-RISICO-INSCHATTINGSMODEL (RRIM)

5

De beveiligingseisen verschillen per ruimte in het gebouw en het verdient dus aanbeveling om hier vooraf enig inzicht in te krijgen. Nu stuiten we spijtig genoeg ook hier weer op het probleem dat er geen gegevens bestaan over de criminaliteitsrisico's. Zoals al eerder aangekaart (zie hoofdstuk 3) zit er in zo'n geval dan niets anders op dan rekening te houden met alle *mogelijke* risico's. Het zal duidelijk zijn dat we daarmee de deur wijd openzetten voor geldverspilling.

Het lijkt ons dan ook het beste om voor elk kantoorgebouw te komen tot een beveiligingsplan waarbij de *mogelijke criminele risico's* enigszins gecorrigeerd worden door middel van een subjectieve inschatting van de *kans* dat een risico zich voordoet en de *gevolgen* die optreden als het (mogelijke) risico zich toch voordoet.

Ten behoeve van dit soort vooraf te maken 'berekeningen' presenteren we een 'Ruimte-risico-inschattingsmodel' (RRIM).

Met dit instrument kan de ontwerper in een gesprek met de opdrachtgever komen tot een enigszins rationele beveiligingsaanpak en prioriteitsstelling (per ruimte in het gebouw en daardoor/daarna voor het hele gebouw).

De basisgedachte achter het RRIM is, dat expliciet bij de (ver)bouw van een kantoor rekening wordt gehouden met het ontwerp beveiliging. Het RRIM bestaat uit een matrix die de ontwerper samen met de opdrachtgever per regel moet invullen. Na invulling zal de *opdrachtgever* de knopen moeten doorhakken. Wat beveiligen we wel en wat beveiligen we niet meer. We verwijzen hierbij naar de beschouwing over 'risk management' in het begin van hoofdstuk 3. De keuze niet-beveiligen maar wel verzekeren kan een reële zijn. Die keuze mag – en kan – de ontwerper echter nooit maken. Anderzijds mag de ontwerper de opdrachtgever de uitkomst van zo'n keuze ook niet opdringen (door beveiliging in het ontwerp niet 'in te bouwen', dwingt de ontwerper de opdrachtgever bijvoorbeeld tot de keuze 'verzekeren' of 'niets doen en er maar het beste van hopen').

HET RRIM

Het RRIM bestaat uit acht kolommen.* De invulling van de matrix start met het in de eerste kolom neerzetten van alle ge-

bouwonderdelen. Onder de term gebouwonderdelen verstaan we hier ruimtes binnen het gebouw (computerruimte, entree, kantoor, leidingschachten enz.; zie voor een overzicht het volgende hoofdstuk). Achter elk gebouwonderdeel (ruimte) in de eerste kolom vult men vervolgens per regel de volgende zaken in:

2 *Toegankelijk* voor ... (welke 'groep' mensen: bijvoorbeeld werknemers, publiek, bezoekers);

3 Het *mogelijke risico*: let wel: het gaat hier om wat er (bij wijze van spreken in het ergste geval) qua criminaliteit zou *kunnen* plaatsvinden.

4 De *kans* dat genoemd risico ook echt plaatsvindt. Het gaat hier om een subjectieve inschatting (gebaseerd op ervaring, horen zeggen, in de krant gelezen enz.). Het is hier de kunst om niet al te optimistisch, maar ook niet al te pessimistisch te zijn. De kans kan men aangeven door middel van een letter tussen de A en de J. Een A voor een grote kans en een J voor een kans die gelijk is aan 0 enz.

5 De *ernst* van de *gevolgen als* het mogelijke (!) risico (zie kolom 3) inderdaad plaatsvindt. Deze kolom kan men desgewenst nog uitsplitsen in:

* = Een vergelijkbare methode is te vinden in Green, 1987/hoofdstuk 7 en Healy en Walsh 1971/17.

* = U ziet: zo'n gevolg lijkt de conclusie te wettigen dat er dus zwaar beveiligd moet worden; onzes inziens is dat echter een onjuiste conclusie: de administrateur kan bijvoorbeeld ook elke avond een back-up mee naar huis nemen.

- materiële schade (de kosten van het verlies, herstelkosten, produktievertraging enz.);
- immateriële schade (angst bij personeel, reacties van klanten, gezichtsverlies enz.).

Zo'n uitsplitsing hebben wij in het volgende voorbeeld overigens niet toegepast om het niet nog ingewikkelder te maken.

In deze 'ernst-van-gevolgen'-kolom kan men een getal tussen de 1 en de 10 neerzetten.

Een 1 als de gevolgen qua ernst desastreus zijn; bijvoorbeeld als het gevolg van het aangegeven mogelijke risico is dat de hele debiteurenadministratie verloren gaat.*

Een 10 is op zijn plaats als de ernst van de gevolgen volstrekt onbeduidend is; bijvoorbeeld het geheel in het ongerede ra-

ken van de crediteurenadministratie.

6 De resultaten van kolom 4 en 5: de beveiligingsprioriteit. Het 'getal' in deze kolom ligt ergens tussen de A1 en de J10. Bij een prioriteit van A1 is kennelijk voor de daar genoemde ruimte én de kans heel groot dat een gebeurtenis ook echt plaatsvindt (een A in kolom 4), én zijn de gevolgen als er iets gebeurt desastreus (een 1 in kolom 6). We merken op dat men deze prioriteitskolom nooit heilig mag verklaren. De bedoeling van de kolom is slechts om te laten zien in welke ruimtes van het gebouw de pijn het grootst is. Daar zal dus in ieder geval iets moeten gebeuren.

7 Aanvullende preventieve maatregelen.

Bij de inschattingen zoals die in de voorgaande kolommen gemaakt zijn, heeft men de bestaande beveiligingsmaatregelen

1 Gebouwonderdeel	2 Toegankelijk voor	3 Mogelijk risico
Toegangen		
Verkeersruimten		
Nooduitgangen en trappehuizen		
Kelders		
Technische ruimten		
Leidingkokers		
Magazijnen en archieven		
Postkamer en expeditie		
Computerruimten		
Bewakingsruimten		
Schoonmaakruimten		
Kantoorruimten		
Publicksruimten		
Kantine en recreatieve ruimten		
Gevels		
Daken		
Terrein voorzijde		
Terrein achterzijde		
...		

daarmee ten minste de risico's (en de daartegen in te zetten maatregelen) expliciet gemaakt.* Op basis van dit werk (waarbij het RRIM slechts een stuk gereedschap is) kan vervolgens een hoofdstuk beveiliging in het programma van eisen gemaakt worden. Beveiliging draait dan verder gewoon in het ontwerpproces mee (bestek, uitvoering).

Om de ontwerper en/of opdrachtgever een stap verder te helpen is in het volgende hoofdstuk een overzicht opgenomen van alle ruimten/elementen die in de eerste kolom van het RRIM kunnen worden opgenomen. Per ruimte worden nog zeer globaal enkele punten gegeven die per ruimte/element centraal staan, gevolgd door een verwijzing naar de voor de desbetreffende relevante ruimte bouwtechnische punten die in de daarop volgende hoofdstukken behandeld worden.

* = Gemakshalve spreken we hier steeds over 'de opdrachtgever'. Voor de ontwerper zit er daarbij nog een adder onder het gras: met wie moet hij/zij het RRIM 'doorrekenen'? Het verdient onzes inziens daarbij zeker aanbeveling om de zaak op hoog niveau te regelen (directie, raad van bestuur, facility manager).

Het voorgaande hoofdstuk werd besloten met de presentatie van een matrix waarbij voor elke ruimte in het kantoorgebouw de voor een goed beveiligingsplan benodigde basisgegevens op een rijtje worden gezet. De ontwerper en de opdrachtgever dienen de risico's (en de beveiliging) per ruimte door te lopen, omdat niet alle ruimten dezelfde eisen stellen aan een beveiliging en er ruimten zijn die zelfs zeer specifieke eisen stellen. Daarom volgt hieronder een opsomming van die verschillen en van die speciale eisen.

Het doel van de behandeling van deze ruimten/elementen in dit hoofdstuk is niet meer dan het globaal aantippen van enkele hoofdpunten en ideeën. Per ruimte/element eindigt de korte beschrijving over het algemeen in een verwijzing naar de meer technische detailhoofdstukken en paragrafen in het vervolg van dit rapport. Dit hoofdstuk vormt daarmee in feite een scharnierpunt: van de risico-inschatting naar de ontwerp oplossingen.

RRIM PER RUIMTE/ELEMENT

Welopen de volgende ruimten/elementen bij langs:

- Toegangen;
- Verkeersruimten en trappehuizen;
- Nooduitgangen en noodtrappehuizen;
- Kelders;
- Technische ruimten;
- Leidingkokers;
- Magazijnen en archieven;
- Postkamer en expeditie;
- Kluizen;
- Computerruimten;
- Bewakingsruimten;
- Schoonmaakruimten;
- Kantoorruimten;
- Publieksruimten;
- Kantine en recreatieve ruimten;
- Gevels;
- Daken;
- Terreinen.

Toegangen

Bij het beveiligen van gebouwen is het een van de lastigste zaken, dat er toch altijd mensen in en uit het gebouw moeten kunnen. Het is aan te raden, om zo min mogelijk entrees in een gebouw te maken. Hoe minder entrees, hoe minder plaatsen

in de gaten gehouden moeten worden en hoe beter het overzicht daarover kan zijn. De mogelijkheid om bijvoorbeeld slechts één entree te maken, is echter onder andere afhankelijk van de grootte van een gebouw. Voor een klein kantoor zal dit geen probleem zijn. Bij grote kantoren zal alles gedaan moeten worden om de pieken aan het begin en eind van de dag op te vangen. Dat kan door toch meer entrees te maken waar men met een toegangsbewijs naar binnen mag. Daarnaast kunnen natuurlijk organisatorische maatregelen worden overwogen, zoals bijvoorbeeld variabele werktijden. Het probleem wordt nog groter, als men bij de deur ook nog wil controleren of de mensen wel gerechtigd zijn om het pand te betreden. Daarvoor stond er vroeger een portier bij de deur. Maar er zijn in de loop der jaren diverse systemen ontwikkeld om de toegangscontrole te beheersen, vanaf eenvoudige kaarten met een pasfoto tot en met ingenieuze systemen, die verschillende biometrische kenmerken van mensen, zoals het gewicht of de lengte/breedteverhouding van een vinger, kunnen meten. Een nadere opsomming van deze systemen wordt in hoofdstuk 9 gegeven, we beperken ons hier tot de grote lijn. Een belangrijke beslissing bij de keuze van de soort entree is, waar mensen moe-

*Toegangen nieuw ...
... en oud*



ten worden tegengehouden of gecontroleerd. Dat zou bij de poort kunnen zijn, zodat bij het gebouw niets meer hoeft te gebeuren. Het zou ook meteen aan de schil van het gebouw kunnen gebeuren, zodat het zonder toegangsprivilege gewoon niet mogelijk is om het gebouw binnen te komen. Maar het kan ook binnen het gebouw zijn, zodat men bij de controle in elk geval droog staat. Indien in een gebouw meerdere gebruikers kantoor houden, die geen gezamenlijke controle uitoefenen, kan het nodig zijn om de controle bijvoorbeeld per verdieping te doen en derhalve wel toegang toe te staan tot trappen en liften. Voor het toezicht is dit echter een slechte oplossing. Hoe dieper een onverlaat het gebouw binnendringt, hoe moeilijker ook om handelend op te treden. Al het bovenstaande geldt voor die tijd, dat een gebouw in bedrijf is. Voor de tijd dat het gebouw dicht is, moet een entree voldoen aan de eisen zoals die zijn genoemd in hoofdstuk 7 (Inbraakbeveiliging).

Voor gebouwen die ook een publieksfunctie hebben, kan een eenvoudige stelregel worden gehanteerd. De publieksruimten en de werkruimten moeten altijd worden gescheiden en ook zullen de beide gebieden een eigen entree moeten hebben. De

gebieden waar de werknemers en de bezoekers elkaar ontmoeten, zullen nauwkeurig moet worden ontworpen en gedetailleerd, afhankelijk van de mate van te verwachten onvriendelijkheden of van mogelijke pogingen tot geweld, roof of ontvreemding.

Verkeersruimten en trappehuizen

Als bij de ingang van een gebouw reeds controle heeft plaatsgevonden, zal er nauwelijks reden zijn om de hoofdverkeersruimten ook nog te voorzien van afgesloten deuren of sluisen. Wel kunnen nog gebieden worden genoemd, die apart zijn beveiligd; zie hiervoor verder ook hoofdstuk 8: Compartimenteren.

Daarbij kan worden gedacht aan computerruimtes, aan kluizen of aan de kantoren van de Raad van Bestuur. Deze gebieden kunnen een apart toegangsprivilege vereisen. Dit zal bij voorkeur moeten gebeuren in combinatie met het eerder genoemde systeem, om te vermijden dat een veelheid aan kaarten of badges ontstaat. Als er ook hier een portier aanwezig is, is onderling contact tussen de verschillende beamtten aan te raden. Als nog niet eerder controle is uitgeoefend en dit na de trap of lift of na de hoofdverkeersruimte wel het geval



moet zijn, moeten deze ruimtes zo overzichtelijk mogelijk gemaakt worden en zo min mogelijk plaats bieden om zich op te houden. Het valt te overwegen om die ruimtes, in combinatie met de hoofdentree, toch op een of andere manier zichtbaar te maken, bijvoorbeeld met een gesloten televisiecircuit, zodat in elk geval de mogelijkheid bestaat om iets waar te nemen. Dit is overigens alleen zinvol als



er ook kan worden ingegrepen. De schaal van het gebouw en de verkeersgebieden spelen daarbij een rol.

Net als bij de entrees geldt, dat bezoekers en werknemers altijd gescheiden moeten blijven. Als er geen beperkte bezoekersruimte, horizontaal en verticaal, kan worden gemaakt, zullen liefst ook dubbele trappehuizen moeten worden gemaakt. Bij bescheiden bezoekersaantallen hoeft dit niet op te gaan, maar dan moet het risico goed worden afgewogen tegen het mogelijke ongemak en de kosten.

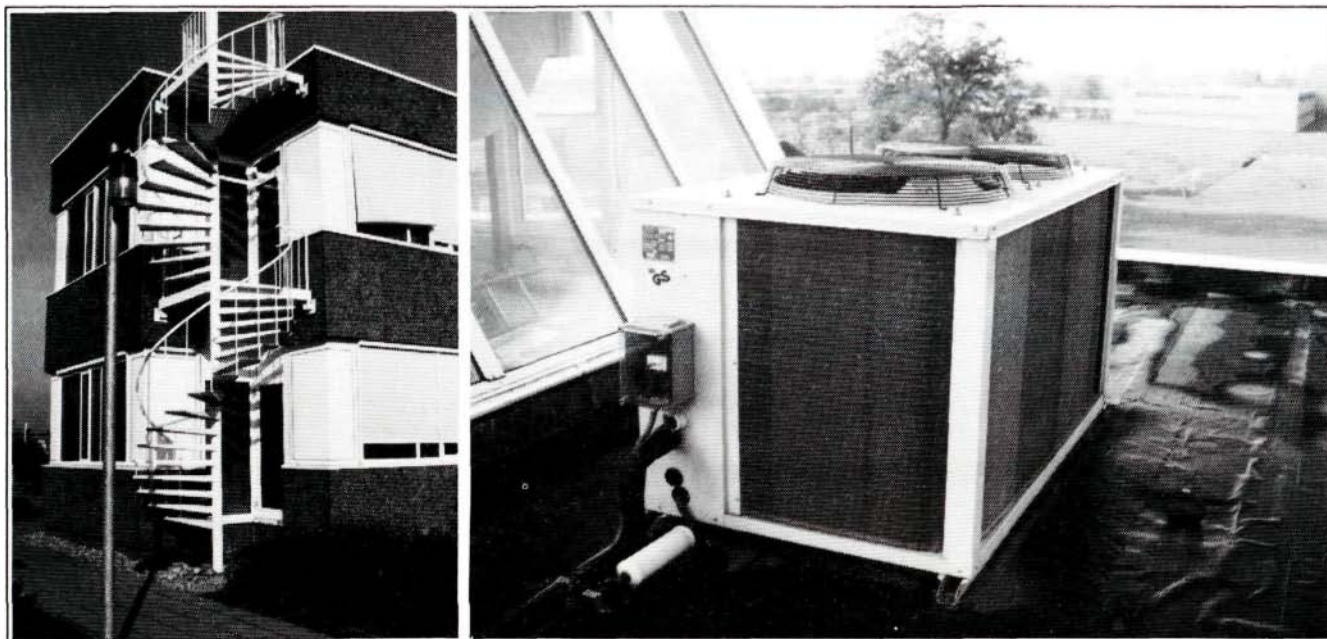
Nooduitgangen en noodtrappehuizen

Veel van wat geldt voor de gewone ingangen, uitgangen en trappehuizen, geldt evenzeer voor de nooduitgangen. Daarbij moet goed worden bedacht om welke redenen ze zijn gemaakt c.q. door wie ze zijn vereist. Doorgaans zullen ze namelijk gemaakt zijn op last van de brandweer om in geval van brand het personeel snel langs meerdere wegen af te kunnen voeren. Het aantal in/uitgangen wordt daarmee echter vergroot en het wordt ingewikkelder ze te controleren. Bovendien moeten de nooddeuren altijd zodanig worden afgesloten dat ze in geval van nood altijd voor iedereen van binnenuit te openen zijn. Zie voor de bouwkundige details verder hoofdstuk 7 en 10.

Het is mogelijk — en vrijwel altijd gebruikelijk — om de noodtrappehuizen ook te gebruiken als dagelijkse verbinding tussen de verdiepingen. Als men dit wil vermijden, wordt welgekozen voor de 'oplossing' om het trappenhuis buiten het gebouw te plaatsen, al of niet in de open lucht. Daardoor ontstaat de noodzaak om op elke verdieping een nooddeur te maken. Hierdoor neemt het aantal aandachts- en ook probleempunten van het gebouw toe. Daarnaast zijn met name de open buitentrappen veelal een eldorado voor jeugdige klimmers en onderzoekers, misschien bij gebrek aan andere uitdagende klimobjecten in de buurt. Een en ander brengt ons in ieder geval tot de aanbeveling om in een ontwerp afscheid te nemen van de open nood-buitentrap.

links:

Simpele scheiding tussen bezoekers en werknemers



Open vluchtttrap: af te raden ... en ... de daksituatie die daarop aansluit

Kelders

Doorgaans zullen in kelders geen werkruimtes, in de zin van kantoorruimtes, worden gevonden. Wel zullen magazijnen, archieven en parkeergarages worden aangetroffen. Het is zaak deze ruimtes te ontsluiten via de normale entree of, indien dat niet mogelijk is omdat men met een auto binnen moet kunnen rijden, een aparte inrit te maken. Deze zal zoveel mogelijk afgesloten moeten zijn en vanuit de hoofdentree moeten worden bewaakt en/of overzien. Daarnaast kan aan mensen een toegangskaart worden gegeven, waarmee men kan binnenkomen. Dit systeem zal bij voorkeur in relatie met het mogelijke hoofdtoegangssysteem werken en zo zal men dan ook via bijvoorbeeld een parkeergarage het gebouw kunnen betreden zonder eerst weer naar buiten te hoeven. Voor toeleveringsbedrijven, bezoekers en dergelijke, zal toegang slechts zijn toegestaan met een speciale goedkeuring.

Technische ruimten

Technische ruimten van een gebouw zijn de ruimten waar de ketel van de centrale verwarming staat en waar de andere in-

stallaties zijn ondergebracht. Deze ruimten zullen meestal gewoon afgesloten zijn en niet toegankelijk zijn voor anderen dan zij die er echt iets te maken hebben. Er zullen dan meestal ook geen extra maatregelen nodig zijn.

Leidingkokers

Voor zowel de normale installaties, werktuigkundig en elektrotechnisch, in het gebouw, als voor speciale beveiligingssystemen, zijn kokers en goten nodig. De horizontale en de verticale doorgangen zijn nodig, plus de nodige systemen om een en ander in aan te leggen. Gezien de grote diversiteit van de leidingen en het gegeven dat sommige leidingen in geen geval direct naast elkaar mogen liggen, moet vooral voldoende ruimte worden gereserveerd. Daar komt bovendien bij, dat toekomstige veranderingen in de systemen met enig gemak moeten kunnen worden uitgevoerd en ook dat interne veranderingen in de verschillende kantoorruimten moeten kunnen plaatsvinden. Over alle mogelijke veranderingen in verlichting, communicatiesystemen en gebruik van computersystemen, kan een apart boek geschreven worden. Dat zullen we maar overlaten aan specialisten op

die terreinen, maar het tempo waarin in het jongste verleden reeds veranderingen mogelijk zijn gebleken, rechtvaardigt in elk geval de aandacht voor mogelijke veranderingen. De flexibiliteit van zowel de ruimten als de installaties moet worden ingebouwd. Na elke verandering zullen leidingkokers en dergelijke op voldoende wijze brand- en inbraakpreventief gecompartmenteerd moeten worden.

Magazijnen en archieven

Voorzover magazijnen en archieven nodig zijn voor het echte kantoorwerk en niet voor opslag van te verkopen voorraad, zal weer aandacht moeten worden besteed aan de toegang, als deze direct vanaf buiten mogelijk is. Van binnenuit zal slechts een beperkt aantal werknemers iets te zoeken hebben in deze ruimten. Daarom kan vaak worden volstaan met goed hangen en sluitwerk en met een goed slot of kan worden doorgeborduurd op het andere toegangssysteem. Buiten werktijd zullen de ruimtes goed afgesloten moeten zijn. Het zal vaak mogelijk zijn om de ruimtes zonder veel ramen te maken, zodat daar dan ook geen extra aandacht aan hoeft te worden besteed. Zie verder voor bouwtechnische details archiefruimten hoofdstuk 8.

Postkamer en expeditie

Voor postkamer en expeditie geldt in het algemeen hetzelfde als voor magazijnen en archieven (zie dus ook hoofdstuk 8).

Kluizen

Een kluis is eigenlijk niets anders dan een magazijn voor waardevolle artikelen of geld. Aan zowel de wanden als de deuren worden dan extra eisen gesteld, afhankelijk van de weerstand die ze moeten kunnen bieden aan brand, inbraak enz. Bij hogere eisen zal overgegaan moeten worden tot een meer speciale bouwkundige oplossing met een kluisdeur. Er kan sprake zijn van tijdens de bouw gemaakte kluizen, maar tegenwoordig bestaan er ook



Kluisdeur

geprefabriceerde kluiselementen, die bepaalde voordelen bieden ten opzichte van in het werk gestort beton. Het is noodzakelijk om de kwaliteit goed te omschrijven, zodat noch een te zware (en meestal dure) noch een te lichte uitvoering wordt gekozen.

De kluis is toegankelijk voor slechts een klein aantal gelukkigen; soms zelfs voor maar één persoon, bijvoorbeeld afhankelijk van het slot. Dit kan een slot met een geheime cijfercombinatie zijn, maar ook een kluis slot of een slot met een dubbele afsluiting. Zie verder voor bouwtechnische details kluisruimten hoofdstuk 8 en voor brand- en inbraakwerende kasten hoofdstuk 8.

Computerruimten

Er zijn verschillende soorten computerruimten, die elk hun eigen eisen hebben. Als er sprake is van een rekencentrum of een 'zenuwcentrum' van een bedrijf, zal het doorgaans de bedoeling zijn om deze ruimten beperkt (gecristreerd) toegankelijk te maken. Dit kan bijvoorbeeld door middel van een op het algehele systeem aansluitend toegangsbewijs, voor de mensen die daar werken. Daarnaast kan de wens bestaan om de functie goed tegen

inbreuk van buiten te beschermen door alle ramen en deuren op z'n minst te voorzien van slagwerend glas, door ramen afsluitbaar te maken en door alle bewegende delen te voorzien van goed hang- en sluitwerk. Bovendien kan worden overwogen om buiten werktijd een inbraaksignaleringsysteem toe te passen. Het principe van dit soort systemen wordt behandeld in hoofdstuk 7. Behalve het volledig afscheiden van computerruimten, hetgeen alleen incidenteel zal voorkomen, zal in toenemende mate de wens bestaan om een ruimte beschikbaar te hebben waar software en banden/schijven kunnen worden opgeslagen. Zie voor 'data-archieven' en 'data-kluizen' hoofdstuk 8.

Bewakingsruimten

In elk gebouw dat op een of andere manier wordt bewaakt, zal een ruimte nodig zijn om apparatuur en/of mensen onder te brengen. In veel gevallen wordt een combinatie gezocht met een ontvangst- of balie functie bij de ingang van een gebouw. Er is dan soms sprake van een heel open situatie, soms van een zeer gesloten portiersloge. Naast deze balie of loge, zal vaak nog een tweede ruimte nodig zijn om

de functie over te nemen buiten werktijd of als dubbel van de eerstgenoemde plek. Soms is het verstandig dergelijke ruimten van een pantry en toiletten te voorzien.

Indien een bewakingsruimte wordt gemaakt, moet deze dicht bij het te bewaken deel van het gebouw, meestal de ingang, liggen. Als ook de nachtdienst wordt verricht in een ruimte, moet gezorgd worden dat buitenstaanders geen zicht op de ruimte hebben. Dit geldt in mindere mate voor overdag en is zelfs onmogelijk als tevens bezoek moeten worden binnengelaten en doorverwezen. Zie verder voor bouwtechnische details hoofdstuk 8.

Schoonmaakruimten

Voor de schoonmakers van een gebouw zal, afhankelijk van de grootte van het gebouw, een aparte ruimte nodig zijn waar men zich kan verkleeden en wassen en waar gerust kan worden. Voor een gebouw dat wordt bewaakt zullen steeds goede afspraken gemaakt moeten worden over de tijd waarop schoonmaakwerkzaamheden worden verricht. In dit verband vragen de ruimten die (extra) zijn afgesloten om bijzondere aandacht. Hiervoor moeten speciale maatregelen worden genomen, bijvoorbeeld door deze

Balie, gezien vanuit de voor het publiek toegankelijke ruimte



ruimten te laten reinigen onder werktijd of door toegangsprivileges te geven aan de schoonmakers, of de schoonmaakwerkzaamheden onder toezicht te laten uitvoeren.

Kantoorruimten

Over het algemeen zal er voor de gewone dagelijkse werkzaamheden geen extra bewaking nodig zijn, zeker niet als er al sprake is van een toegangscontrole bij de ingang van het gebouw. Het lijkt zelfs af te raden om veel ruimten extra te beveiligen, omdat dit voor de werknemers altijd last mee zal brengen en dan tot ontduiking van een systeem zal leiden. Beveiliging kan alleen effectief zijn als iedereen overtuigd is van het nut en bereid is mee te werken. Als de noodzaak bestaat om bepaalde (bij voorkeur gegroepeerde) ruimten wel te beveiligen, zal dat deel of zullen die delen van het gebouw goed moeten worden afgesloten van de overige ruimten. Bij de entree(s) van het beveiligde gebied kan weer gevraagd worden om het toegangsbevijs, aansluitend op andere systemen. Speciale aandacht moet worden besteed aan mogelijke omwegen, bijvoorbeeld via trappehuizen en/of noodtrappen. Deze zullen moeten worden afgesloten, of in elk geval slechts eenzijdig toegankelijk moeten zijn.

Publieksruimten

Zodra een deel van het kantoor vaak wordt bezocht door veel publiek, moet daarmee van het begin af aan terdege rekening worden gehouden. Het verdient in principe aanbeveling om een strikte scheiding te maken tussen ruimten voor het publiek en ruimten waar het publiek niets te zoeken heeft. De mate van de scheiding wordt vooral uitgedrukt in de stevigheid en de hoogte van de afscheiding, variërend van een eenvoudige balie of deur tot een volledig met kogelwerend glas beveiligd loket. Het is goed om de toegang voor werknemers te scheiden van de toegang voor publiek. Bij kantoren waar bezoek naar werkruimten moet worden geleid,

wordt het steeds gebruikelijker om bij binnenkomst de naam van de bezoeker en het doel van het bezoek te noteren en daarna, bij het verlaten van het pand, de bezoeker uit te schrijven. Daarmee worden niet alleen ongewenste gasten geweerd, maar er kan ook een controle worden uitgeoefend op het aantal aanwezige mensen in het pand.

Kantine en recreatieve ruimten

Voorzover de kantine en de recreatieve ruimten onder werktijd worden gebruikt, hoeven geen speciale eisen te worden geformuleerd. Wel bestaat de mogelijkheid om een toegangscontrolesysteem te combineren met een tijdbestedingscontrole, waarvoor bij deze ruimten een aan- en afmeldpost nodig kan zijn. Als de ruimten ook buiten de normale werktijden moeten worden gebruikt, is het te overwegen om ze geheel buiten de gecontroleerde ruimten om toegankelijk te maken. Het is dan ook nodig alle secundaire ruimten als bijvoorbeeld toiletten bereikbaar te maken of dubbel uit te voeren. Deze situatie zal zich eerder voordoen bij de grotere kantoren dan bij de kleine, maar het kan nodig zijn voor personeelsavonden, voor de bedrijfsklaverjasclub enz. De ervaring leert dat de kantine bij inbraak doorgaans een grote belangstelling geniet. Het is derhalve raadzaam hier een elektronische inbraaksignalering toe te passen.

Gevels

Waar een kantoor ook staat, wat er ook gebeurt en hoe groot of hoe klein het is, het zal altijd nodig zijn om inbrekers te weren. Het is dus altijd nodig om de ruimten op de begane grond en de bereikbare ruimten op de verdiepingen zodanig van de buitenwereld af te sluiten, dat inbrekers een beperkte kans hebben om binnen te komen. Allereerst moet dus degelijk hang- en sluitwerk op alle bewegende delen op de begane grond worden toegepast en eventueel op de eerste verdieping als hier bereikbare plaatsen zijn. Verder verdient het aanbeveling om minstens slag-



*Fraai ogende
glasafscherming*

werend glas toe te passen in raamopeningen op de begane grond. Zeker als gevelopeningen zich op minder goed zichtbare plaatsen in het gebouw bevinden, verdient glasafscherming aanbeveling: zowel aan de binnen- als aan de buitenzijde van het glas kan een metalen bescherming worden aangebracht. Dit kan op een klassieke manier, maar ook op een meer artistieke wijze uitgevoerd worden.

Het zal duidelijk zijn, dat niet alleen de ramen van deugdelijk materiaal moeten zijn; de gehele plint van het gebouw moet van gladde, stevige materialen worden opgetrokken. Naast de stevigheid gaat het ook om het onderhoudsgemak van de materialen en zonodig om het gemak van vervanging. In gebieden met veel graffiti zullen bovendien nog extra maatregelen nodig zijn, zoals bijvoorbeeld het aanbrengen van een anti-graffiti-coating, waardoor graffiti tamelijk eenvoudig te verwijderen is. Als men in de avonduren een actieve bewaking bij het gebouw heeft, waarbij aandacht wordt besteed aan de directe omgeving van het gebouw, zal het aanbeveling verdienen om goede verlichting aan te brengen, om camera's te posteren en om een strook om het gebouw vrij te laten om het zicht mogelijk te maken.

Deze maatregelen worden verder behandeld in deel 5 van deze serie Beveiliging van gebouwen. Zie voor inbraakwerende gevels hoofdstuk 7 en voor vandalisme en brandstichtingspreventie hoofdstuk 12.

Daken

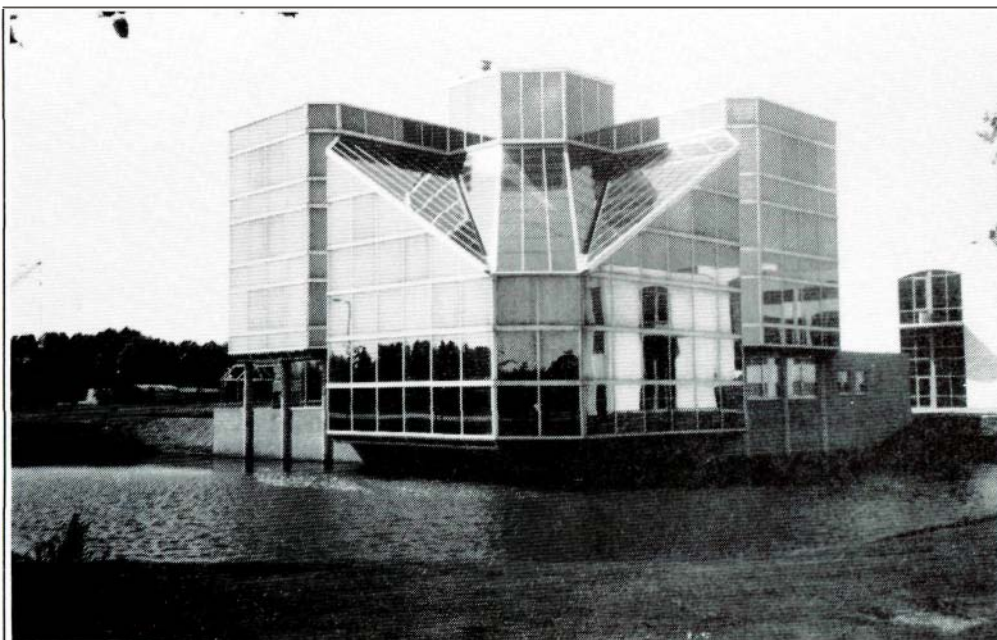
Voor vrijstaande gebouwen zal hier geen extra aandacht nodig zijn, maar met name



in stedelijke gebieden zullen aan daken dezelfde eisen aan inbraakveiligheid worden gesteld als aan gevels. Voorkomen moet worden, dat men zich via aanpalende panden toegang tot het gebouw kan verschaffen. Zie verder voor bouwtechnische details hoofdstuk 7.

Terreinen

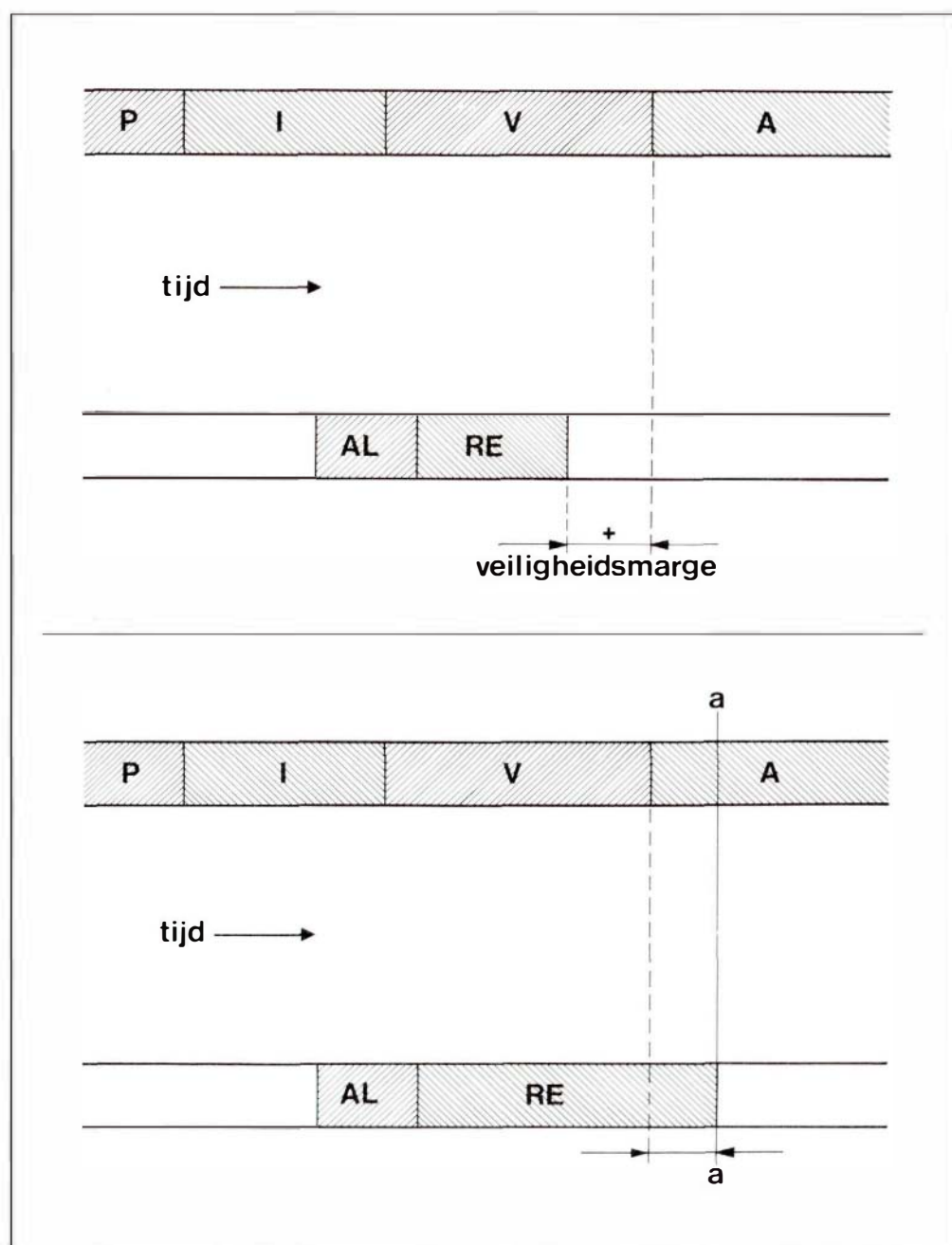
Over het algemeen zal er niet vaak sprake zijn van bij een kantoor behorende terreinen en parkeergarages. De eisen die toch te stellen zijn, zoals bijvoorbeeld met betrekking tot opslag of overslag, overzichtelijkheid, verlichting enz., zullen (naast hetgeen in hoofdstuk 11 wordt opgediend) worden behandeld in het vijfde deel van de serie Beveiliging van gebouwen. Daarbij zal dan ook uitgebreid aandacht worden besteed aan hekwerken, poorten, terreinvormen, beplanting, vijvers, grachten enz.



links:
Technische afscherming
(hekwerk)
rechts:
Natuurlijke afscherming
(water)

PIVA-ALRE-theorie:

*Hier een positieve
veiligheidsmarge*



*Negatieve
veiligheidsmarge*

Eén van de meest voorkomende risico's waartegen kantoorgebouwen beveiligd dienen te worden is inbraak. Inbraakbeveiliging is niet alleen – zoals de beveiligingsindustrie nogal eens wil doen geloven – het installeren van elektronische detectie-apparatuur. Het moet een planmatige totaalaanpak zijn in de vorm van een beveiligingsplan met organisatorische en fysieke middelen, waarbij elektronika een noodzakelijke completerende functie vervult.

GEVELS, KOZIJNEN, RAMEN EN DEUREN

Voordat een inbreker door de gevel, het dak of de vloer binnendringt, probeert hij het eerst op gemakkelijker plaatsen, zoals deuren, ramen of andere gevel- en dakopeningen. Vooral *deuren* zijn een geliefd aanvalsdoel, omdat die een aantal voordelen hebben:

- Dankzij het doorgaans slechte hang- en sluitwerk breek je gemakkelijk, snel en nagenoeg geruisloos in.
- Als je via een deur binnenkomt, ben je bij eventuele verrassingen in het gebouw er ook snel weer uit.
- Via een deur voer je doorgaans ook gemakkelijk de buit af.
- Een inbreker die 'rondhangt' bij een deur valt doorgaans niet zo op bij eventuele passanten.

Nu is ook de inbraakbeveiliging van een kantoorgebouw nooit sterker dan de zwakste schakel. Daarom is een belangrijk grondbeginsel dat het kantoorgebouw zo beveiligd moet worden dat in principe een inbraak op elke plaats even moeilijk is. Dat wil niet zeggen dat op alle plaatsen dezelfde beveiligingsmiddelen moeten worden toegepast, maar dat de beveiliging aan de zich ter plekke voordoende 'bedreiging' moet worden aangepast. Om eenzelfde graad van beveiliging te bereiken vereist een bijzonder bedreigde plaats – bijvoorbeeld een slecht in het zicht liggende vluchtdeur aan de achterzijde van een kantoor – dus andere (betere) voorzieningen dan eenzelfde deur aan de goed zichtbare voorkant.

Wanneer deuren om welke reden dan ook

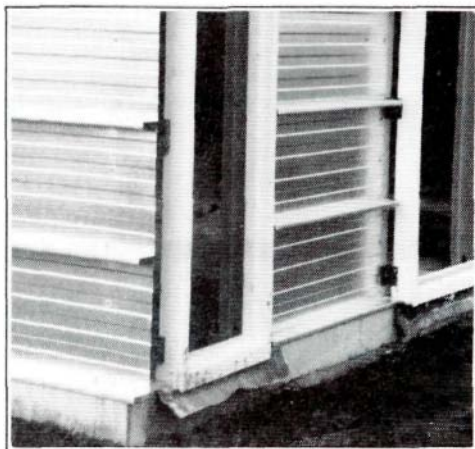
niet in aanmerking komen voor inbraak, bieden ramen vaak voldoende keus. We maken hier onderscheid tussen vaste en beweegbare ramen. Op vrij eenvoudige wijze kan een inbreker doorgaans naar binnen komen wanneer hij bij een beweegbaar raam het glas ter hoogte van de raamvergrendeling inslaat. Ook kan de inbreker, al vereist dit iets meer handigheid, door de glassponning steken of door een raamstijl boren. Door vaste ramen of ramen met een goede afsluitbare vergrendeling wordt niet zo vaak ingebroken als men wel aanneemt. Het inslaan van ruiten gaat namelijk met nogal wat lawaai gepaard. Als de inbreker daarna door de ruit naar binnen wil, moet hij eerst nog alle glasresten wegslaan, om te voorkomen dat hij zich verwondt. De kans is ook groot dat hij bij het door het raam klauteren gemakkelijk sporen achterlaat.

Wanneer de prikkel voor inbraak maar groot genoeg is en ramen en deuren goed beveiligd zijn, zal de inbreker overwegen door gevel, vloer of dak te gaan. Zeker als de inbreker ongestoord kan werken, zoals aan een slecht zichtbare achterzijde van een kantoorgebouw, of de aangrenzende ruimten, of vanuit op een plat dak.

Gevels

Gevels die zijn uitgevoerd in gasbetonelementen, geprofileerd stalen bekledingen en dergelijke, bieden een zeer beperkte inbraakveiligheid. Een goede inbraakwerende gevel heeft een sterkte die vergelijkbaar is met steens metselwerk in een hard-grauwe steenkwiteit, gemetseld met een sterke mortel. Scheidingsmuren van compartimenten moeten liefst voldoen aan

Geprofileerde staalplaat (hier gedeeltelijk gemonteerd) biedt weinig inbraakwering



dezelfde kwaliteit of beter (zie hoofdstuk 8: Compartimenteren). Vooral wanneer het 'binnen komen rijden' met een auto tot de serieuze risico's behoort is een borstwering van die sterkte een minimum eis.

Een gevel uit zware beton-elementen opgetrokken vormt een voortreffelijke basis qua inbraakwering

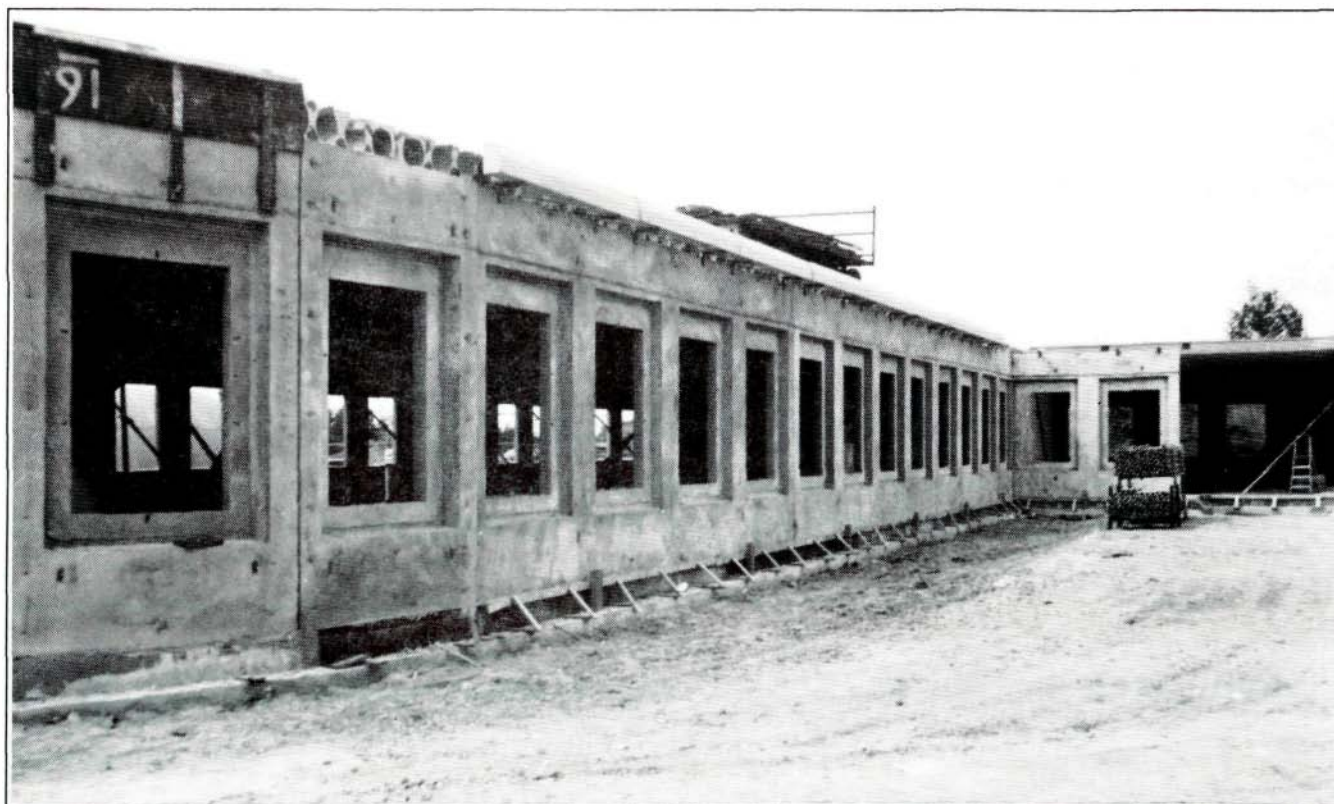
Kozijnen, ramen en deuren

Fysiek beveiligen omvat ook het versterken van het gebouw door het toepassen

van geschikt hang- en sluitwerk en een juiste *inbraakpreventieve detaillering van de gevelopeningen*.

Hedendaagse kwaliteitsverbeteringen op het gebied van onderhoud, isolatie en dergelijke bij vooral nieuwere kozijnmaterialen sluiten niet altijd goed aan op de bedoelde inbraakwerende kwaliteitsverbeteringen. Ernstig wordt de situatie wanneer achteraf blijkt dat uit constructief oogpunt geen enkele inbraakpreventieve maatregel meer kan worden toegevoegd. Een modern kozijn met vaste, draaiende en/of schuivende delen is dus alleen acceptabel wanneer het voldoet aan de eis dat de inbraakwerendheid achteraf door relatief eenvoudige ingrepen nog *kan* worden verbeterd. Dit houdt in dat achteraf nog eens een keer een zwaarder deurttype, dikker (dus zwaarder) gelaagd glas, sluitkommen en dergelijke moeten kunnen worden aangebracht.

In deel 1 van de Beveiliging van gebouwen wordt in hoofdstuk 3 (Keuze-aspecten van kozijnen, ramen en deuren) uitvoerig



op de materialen hout, metaal en kunststof ingegaan. Voor meer informatie op dit punt verwijzen we dus naar deel 1. Samenvattend worden daarin per materiaalsoort de volgende referenties aangehaald:

Hout:

- NEN 3660/61/62, Gevelelementen, ramen en deuren;
- NEN 3665, Gevelvullingen;
- KVT '80 (maart 1986), Kwaliteit van timmerwerk;
- NPR 3670/71/72/73, Gevelvullingen volgens KVT '80 (A t/m C);
- NEN 5088/89, Inbraakwerend hang- en sluitwerk.

Metaal:

- NEN 3660/61/62, Gevelelementen, ramen en deuren;
- VMR, Kwaliteitseisen metalen ramen 1986;
- NEN 5088/89, Inbraakwerend hang- en sluitwerk.

Kunststof:

- NEN 3660/61/62/64, Gevelelementen, ramen en deuren;
- NEN 7034, Profielen ongeplastificeerd PVC;
- NPR 7058, Gevelvullingen ongeplastificeerd PVC;
- NEN 5088/89, Inbraakwerend hang- en sluitwerk.

Samenvattend luiden onze conclusies naar aanleiding van hoofdstuk 3 uit deel 1 dat kozijnen probleemloos inbraakpreventief kunnen worden gedetailleerd aan de hand van deze referenties, al blijken kwaliteitseisen op dit punt voor kunststoffen te ontbreken. Bij toepassing van kunststoffen zal men dus per ontwerp de inbraakpreventieve eisen zelf moeten opstellen. Dat is onhandig en vaak in praktische zin niet uitvoerbaar.

Als we een zeer eenvoudig 'recept' willen presenteren als basis voor een inbraakwerende gevel met gevelopeningen zoals ramen en deuren, dan komen we tot:

- een gevel die is opgetrokken uit steens metselwerk of gelijkwaardig;
- kozijnen die afgestemd zijn op een massieve triplex ('multiplex') deur

(dik ca. 40 mm) met drie-sterren hang- en sluitwerk volgens NEN 5088/89 of gelijkwaardig;

- slagwerend glas in 'binnenbeglazing'.
- Gezien de vele misvattingen op het gebied van slagwerend glas en inbraakwerend hang- en sluitwerk, vatten wij de belangrijkste punten van deze beveiligingscomponenten in dit hoofdstuk 7 nog eens samen. Slagwerend glas en glasafscherming worden zeer uitvoerig behandeld in de hoofdstuk 5 van deel 3 in de serie Beveiliging van gebouwen. Inbraakwerend hang- en sluitwerk wordt uitvoerig behandeld in hoofdstuk 3 van deel 1.

HANG- EN SLUITWERK

De beide normen NEN 5088 en NEN 5089 vormen in Nederland de basis voor het toepassen en goedkeuren van inbraakwerend hang- en sluitwerk:

NEN 5088:

- Inbraakveiligheid van gebouwen;
- Bouwtechnische beveiliging van woningen;
- Toepassing van hang- en sluitwerk.

NEN 5089:

- Inbraakveiligheid van gebouwen;
- Inbraakwerend hang- en sluitwerk;
- Eisen en beproevingsmethoden.

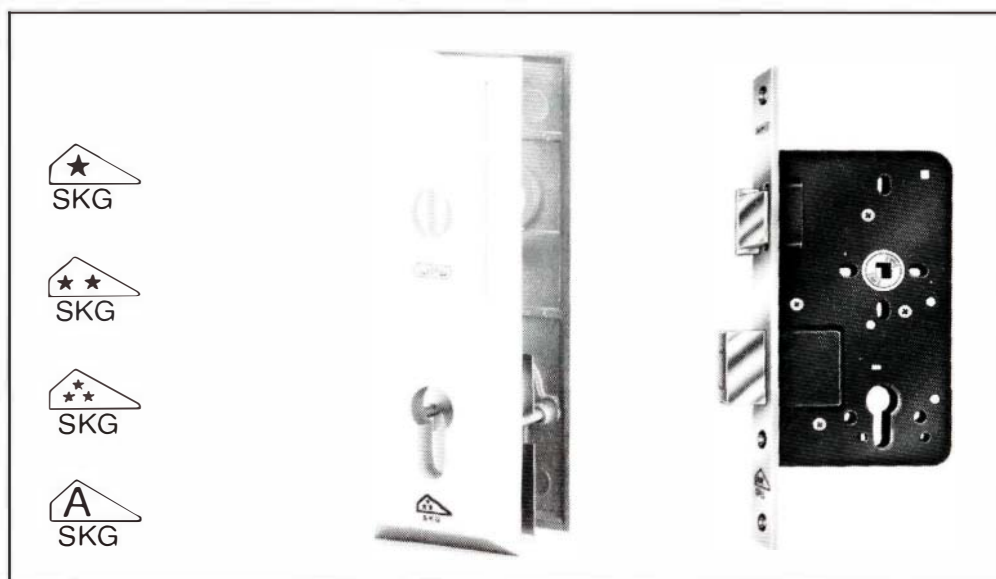
Alhoewel de NEN 5088 toegesneden is op de toepassing bij woningen, kan de norm in principe voor alle typen gebouwen geheel of gedeeltelijk van toepassing worden verklaard. Belangrijk is te weten dat beide normen drie kwaliteitscategorieën kennen:

Categorie	Symbool
STANDAARD	*
ZWAAR	**
EXTRA ZWAAR	***

Kwaliteitsaanduidingen hang- en sluitwerk

In de praktijk wordt naast dit kwaliteitsymbool ook het logo van de keurende instantie onuitwisbaar op de inbraakwerende produkten aangebracht.

*Onuitwisbaar op de
produkten aangebracht
kwaliteitsmerk*



Inbraakwerend hang- en sluitwerk met één en twee sterren wordt veelal in woningen gebruikt, maar voor kantoren dienen in principe altijd drie-sterrenprodukten te worden toegepast. Het mag duidelijk zijn dat naast extra zware hoofdsloten ook extra zware cilinders en overeenkomstig beslag dient te worden toegepast.

De norm NEN 5089 Eisen en beproevingsmethoden geeft uiteraard alle informatie over het verschil tussen de kwaliteitscategorieën. Duidelijk komt het kwaliteitsverschil naar voren bij bijvoorbeeld een zeer

belangrijk slotonderdeel, zoals de nachtschoot.

Het verschil in beproevingskrachten is onderstaande illustratie af te lezen.

GLAS EN GLASAFSCHERMING

Glas

Met glas en/of doorzichtige kunststoffen kan een zekere mate van inbraakwering worden verkregen met behoud van de

*Beproeivingskrachten
in kN*

Categorie	F1	F2	F3	F4	F5	F6	F7
Standaard	3	4	3	7	7	4	3
Zwaar	4	6	4	7	7	6	4
Extra zwaar	5	7	5	7	7	7	5

F3 = drukkracht in langsrichting van de schoot
 F4 = kracht in dwarsrichting van de schoot
 F3 = kracht in zwenkrichting van een zwenkschoot
 F4 = trekkracht op een haakschoot
 F5 = drukkrachten op een sluitkom
 F6 = als F5
 F7 = drukkracht op een scharnier

leefbaarheid in en rond het kantoorgebouw. Indien inbraakwerende beglazing het beoogde effect wil opleveren, zal bij het ontwerp zeer nauwkeurig moeten worden gelet op de volgende punten:

- beglazingssoort en inbraakwerendheid;
- referenties voor inbraakwerendheid;
- sponningdetailering;
- plaatsingsmethode;
- glasbreukdetectie voor inbraaksignalering.

Zoals gezegd wordt in hoofdstuk 5 van deel 3 het onderwerp glas zeer uitvoerig behandeld. We geven aan de hand van bovenvermelde punten zeer in het kort aan wat in dat deel wordt behandeld (zie onder).

Glasafscherming

Allereerst hebben we, zoals we hierboven hebben gezien, de mogelijkheden van de speciale inbraakwerende beglazing: slagwerend glas, glas/kunststofcombinaties en glasconstructies waarbij in de isolerende spouw een inbraakwerend strekmetaalrooster van aluminium (hard) is aangebracht.

Wanneer evenwel normaal (niet-slagwerend) glas in de pui is (of wordt) toegepast, kan de gewenste mate van inbraakwerendheid ook worden verkregen door een doorzichtig slagwerend produkt vóór of achter het glas aan te brengen. We hebben daarbij de keuze uit de volgende

(esthetisch bruikbare) mogelijkheden:

Vóór het glas (aan de buitenzijde):

- A rolluik met beperkt doorzicht;
- B rolhek;
- C panelenluik.

Achter het glas (aan binnenzijde):

- D kunststof folie;
- E tweede ruit van slagwerend glas/kunststof;
- F strekmetaalrooster (staal of aluminium);
- G rolhek;
- H rolluik.

Deze beveiligingscomponenten zijn op pag. 58 afgebeeld en zeer uitvoerig behandeld in hoofdstuk 5 van deel 3.

Kogelwering

Enkele opmerkingen over kogelwering zijn hier op zijn plaats. Ten eerste omdat dit bij kantoren een serieus onderwerp kan zijn, en ten tweede omdat de misvattingen op dit punt vaak groot zijn. Met metalen, glas, kunststof plaat, geweven kunststof materialen, hout en allerlei samengestelde materialen kunnen aanvaardbare kogelwerende constructies worden gemaakt. Hamvraag is natuurlijk waartegen men zich wil beschermen. Van belang zijn daarbij het soort wapen, het soort munitie, de snelheid van de kogel, de trefhoek, de afstand, de temperatuur, enz. Deskundig advies kan men inwinnen bij de fabrikanten en fabrieksagenten van kogelwerende materialen, alswel bij een (be-

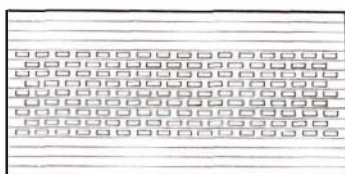
- 1 Een overzicht van de meest voorkomende glas- en kunststofprodukten (en combinaties daarvan), waarbij tevens 'grotweg' de slagwerendheid van die produkten wordt vermeld.
- 2 Een overzicht van de referenties:
 - NL SVB/TBBS Kogel- en kegel-valproef;
 - D DIN 52290: Angriffshemmende Verglasungen, deel 3: Prüfung auf durchbruchhemmende Eigenschaft gegen Angriff mit schneidfähigem Schlagwerkzeug und Klasseneinteilung, deel 4: Prüfung auf durchwurffhemmende Eigenschaft und Klasseneinteilung;
 - GB BS 5544 Specification for anti bandit glazing (glazing resistant to manual attack);
 - USA UL 972 Burglary resisting glazing material.

- 3 Een toelichting op zaken als sponning-hoogte, binnenbeglazing, juiste dikte, consequenties van het hoge gewicht enz.
- 4 Van toepassing zijnde voorschriften van de fabrikant en NEN 3576: Beglazing van kozijnen, ramen en deuren, NEN 3577: Beglazen van gebouwen.
- 5 Een uitleg van de mogelijkheden voor glasbreukdetectie:
 - achteraf aan te brengen glasbreukdetectoren (actief en passief);
 - in het laminaat aangebrachte alarmdraad;
 - 'ingebakken' stroomkring in gehard glas;
 - metallieke opgedampte laag.

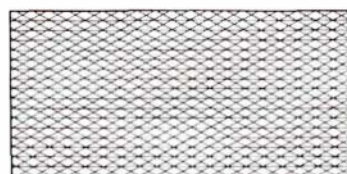
Behandelde onderwerpen omtrent glas in deel 3, hoofdstuk 5

Glasafscherming: vóór of achter het glas aangebracht

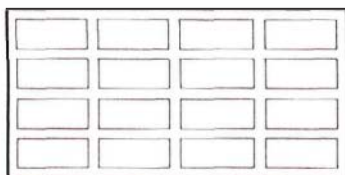
Vóór het glas (aan buitenzijde)



A roluik met beperkt doorzicht

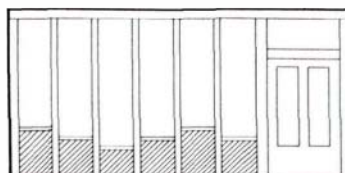


B rolhek

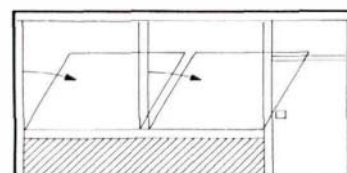


C panelenluik

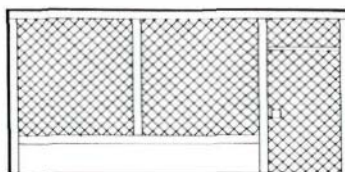
Achter het glas (aan binnenzijde)



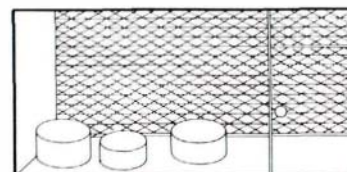
D kunststoffolie



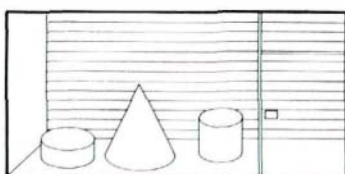
E tweede ruit van slagwerend glas/kunststof



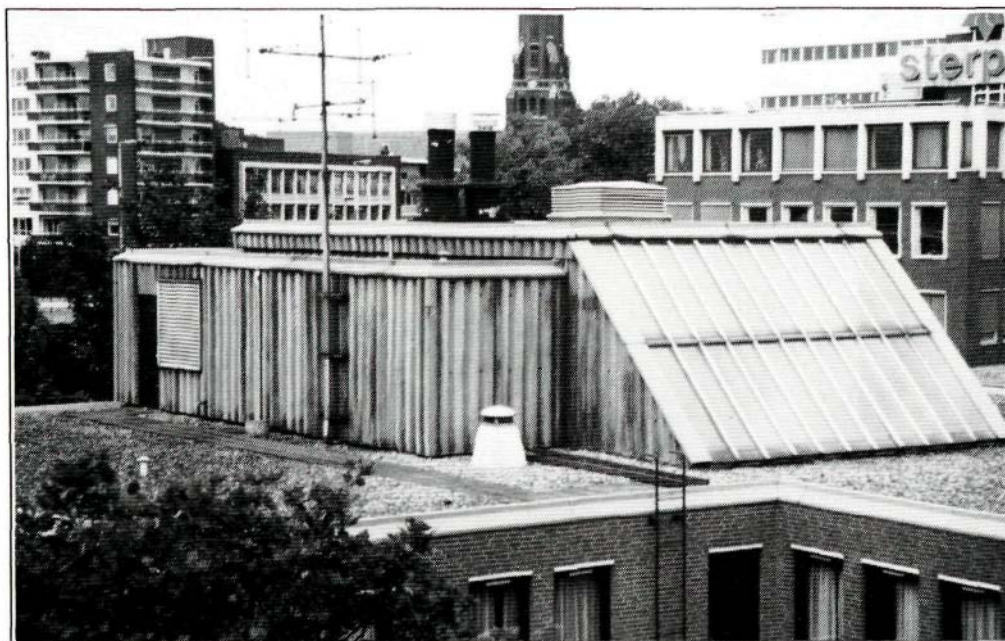
F strekmetaalrooster (staal of aluminium)



G rolhek



H rolluik

*Keet op het dak*

perkt) aantal erkende beveiligingsbedrijven.

De meest voorkomende referenties op dit gebied zijn:

- USA UL 752: Bullet-resisting equipment;
- GB BS 5051: Security glazing, deel 1: binnensituaties, deel 2: Buitensituaties (van -20°C tot $+40^{\circ}\text{C}$);
- D DIN 52290: Angriffshemmende Verglasungen deel 1 en 2.

DAKEN EN VLUCHTWEGEN

Een bezoek op het dak is soms verrassend, vooral als men dit buitenom via de vluchtrappen doet. Enerzijds ontdekt men het gemak waarmee men via de vluchtrap op het dak komt — hetzij via het eigen gebouw, hetzij via belendende gebouwen — en anderzijds verbaast men zich over de bouwsels die men op het dak aantreft.

In de gebouwtjes op het dak bevinden zich veelal de ruimten voor de liften, eindpunten van leidingschachten en trappehuizen, luchtbehandelingsapparatuur en dergelijke, terwijl op grotere platte daken vaak ook nog een veld vol met lichtkoepels wordt aangetroffen. Duidelijk is dat in dit geheel op tal van plaatsen vaak op zeer

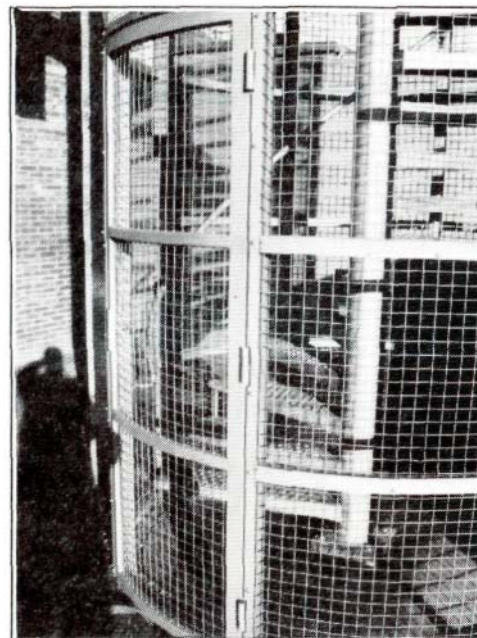
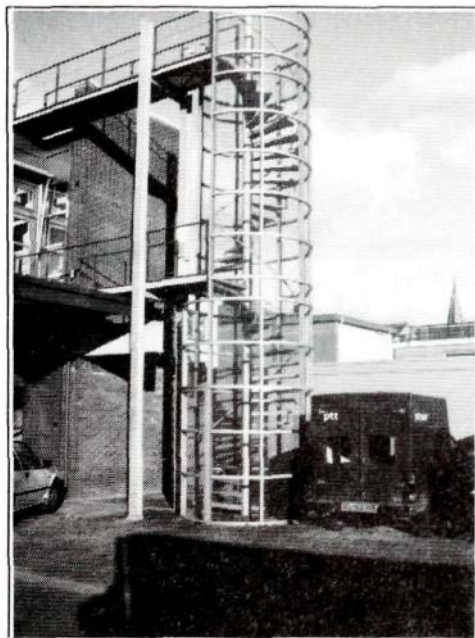
eenvoudige wijze kan worden ingebroken. Om dit risico te verminderen zal in eerste instantie inpandig de toegang tot dergelijke ruimten inbraakpreventief moeten worden gedetailleerd, met behulp van bijvoorbeeld inbraakwerende deuren (40 mm multiplex blad met inbraakwerende scharnieren en een drie-sterren slot o.g.) en inbraakdetectie (ruimtelijk of een reed-contact; zie het laatste deel van dit hoofdstuk).

Bij vluchtrappen buiten het pand zal op de begane grond de toegang tot de vluchtrap moeten worden afgesloten met een kooi. De industrie levert voor dit doel ook esthetisch gezien acceptabele oplossingen; de kooideur is van binnenuit te openen met een kruk, aan de buitenzijde zit 'blind beslag'. Het is zinvol dit soort belangrijke (kooi)deuren mee te nemen in een eventueel aanwezig inbraaksignaleringssysteem.

De dakopbouw zelf dient bij voorkeur in harde materialen te worden opgetrokken, zoveel mogelijk blind met één inbraakwerende deur. Roosters dienen in staal te zijn uitgevoerd en moeten vanaf de buitenzijde niet losneembaar zijn.

De in de dakopbouw en souterrains eindi-

*Vluchttrap afgesloten met
kooi ...
... detail*

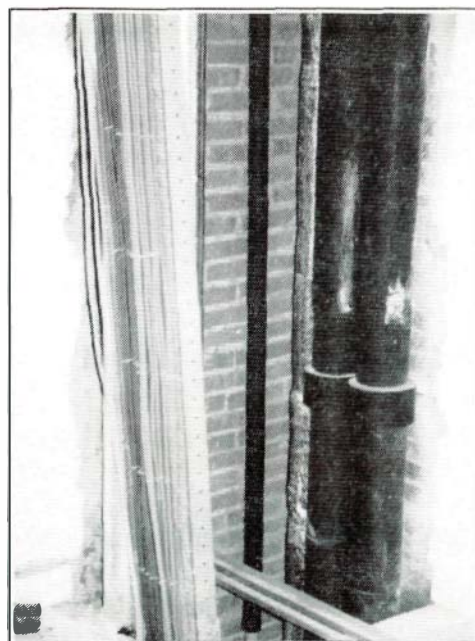


gende leidingschachten vormen door-
gaans de hoofdadrs van de steeds uit-
bundiger wordende netwerken die we in
kantoren aantreffen. De kabels van de
beveiliging lopen daar veelal vrolijk naast.
Het mag duidelijk zijn dat deze schacht-
eindpunten op het dak en in het souter-
rain goed inbraakpreventief moeten wor-
den afgeschermd. In verticale zin zullen
de leidingschachten ook om brandtechni-

sche redenen goed moeten worden ge-
compartimenteerd.

Gevoelige apparatuur op het dak kan op
efficiënte wijze met behulp van een strek-
metaal-afscherming in de vorm van een
kooi worden beveiligd. In de kooi dient
voor servicedoeleinden een luik of deurtje
van strekmetaal te worden aangebracht,
voorzien van een deugdelijke hangslot-
combinatie. Op deze manier wordt de
dakapparatuur eveneens beveiligd tegen
al te nieuwsgierige jeugdige onderzoek-
kers.

*Leidingschacht in
aanbouw*



Lichtkoepels en dergelijke

Lichtdoorlatende openingen op het dak
in de vorm van koepels, lichtstraten enz.
zijn in hun traditionele vorm weinig in-
braakwerend, en dienen aan de onderzij-
de inbraakwerend te worden afge-
schermd met bijvoorbeeld strekmetaal
(aluminium of staal), slagwerend glas of
slagwerende kunststofplaat van bijvoor-
beeld polycarbonaat. De bevestiging van
deze vlakke afscherming onder lichtkoe-
pels en dergelijke kan het beste worden
gerealiseerd met een rondom in de rave-
ling van de balklaag aan te brengen L-pro-
fiel.

De industrie levert ook kunststof licht-

koepels in slagwerende (polycarbonaat) uitvoering met een zeer moeilijk losneembare bevestiging. Ook zijn er slagwerende kunststof lichtkoepels die in de dakbedekking worden 'meegeplakt' waardoor een glad en inbraakwerend geheel ontstaat. Door een veelheid aan goede profielen en blinde bevestigingsmogelijkheden kunnen lichtstraten die worden opgebouwd uit vlakke of gebogen slagwerende plaatmaterialen tegenwoordig op voldoende inbraakwerend niveau worden uitgevoerd, dit in tegenstelling tot de op dit punt min of meer beruchte constructies met draadglas.

Dakmateriaal

Wanneer dakopeningen in platte daken in voldoende mate bouwkundig zijn beveiligd blijft natuurlijk het risico over van het inbreken door het dakmateriaal heen; een in de praktijk niet-onbekende wijze van inbraak. Afhankelijk van de dakconstructie en de risico-situatie zal dan moeten worden overwogen ook het dak aan de onderzijde (voor een deel) af te schermen met daarvoor geschikte plaat- of roostermaterialen.

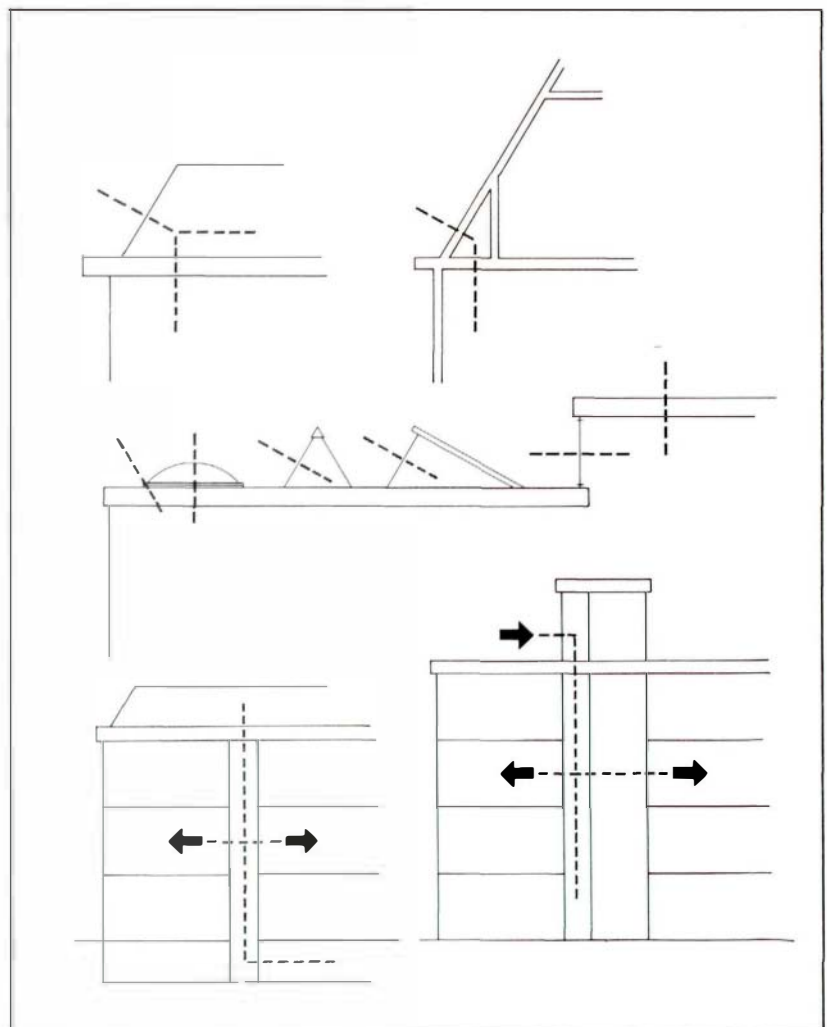
Vluchtwegen

Tegengestelde functies hebben deuren die inbraakwerend moeten zijn uitgevoerd, maar ook zeer gemakkelijk (van binnen-uit) geopend moeten kunnen worden, omdat ze een verplichte vluchtwegfunctie hebben. Dit laatste levert tijdens de opstelling van kantoren vaak het probleem op van het illegale gebruik van deze vluchtdoors door zowel bezoekers als kantoorpersoneel. Na sluitingstijd moeten deze deuren een inbraakwerende functie hebben, hetgeen relatief eenvoudig valt te realiseren door een inbraakwerende deur toe te passen die aan de buitenzijde geheel blind is afgewerkt en aan de binnenzijde is voorzien van een duidelijke panieksluiting. Bij deze vrijwel altijd naar buiten draaiende deur moeten voorzieningen worden getroffen tegen inbraak aan de hangzijde in de vorm van

bijvoorbeeld scharnierbeveiligers. Dit in principe toch eenvoudige recept voor een goede vluchtdoors blijkt in de praktijk maar al te vaak moeilijk uitvoerbaar te zijn. Zo zien we dat deurbladen worden toegepast met een reeds uitgefreesd gat voor de slotkast van een insteekslot, terwijl dat slottype vanwege de anti-panieksluiting helemaal niet wordt toegepast. Dit loze slotkastgat wordt meestal afgewerkt met een traditioneel stel blinde schilden, hetgeen het manipuleren van de panieksluiting van buitenaf wel erg eenvoudig maakt. Dit euvel komt bij veel éénzijdig te bedienen deuren voor, ook wanneer in plaats van een panieksluiting een aan één zijde te bedienen insteekslot wordt toegepast.

In plaats van het gebruikelijke en vaak

*Inbraakgevoelige
daksituaties*



slecht functionerende uitbundige stangenstelsel dat als panieksluiting dienst moet doen, biedt vooral bij kantoren de elektrisch bedienbare paniekbalk ('push-bar') met 'status-informatie' (deur open of dicht, schoot geheel uit of in, enz.) uitstekende mogelijkheden de totale problematiek van *illegaal gebruik* (kantoor geopend), *inbraakwerendheid* (kantoor gesloten) en het voldoen aan de *veiligheidsvoorschriften* van overheden, goed en vormschoon op te lossen.

In de literatuurlijst is het rapport Nooddeuren (uitgave TBBS) opgenomen. Dit rapport gaat uitvoerig in op de uitgangsen toegangsbeheersing van nooddeuren in het kader van de brandbeveiligingsverordening.

INBRAAKSIGNALERINGS-SYSTEMEN

Functie

In kantoren zien we steeds vaker dat inbraakalarmsystemen worden toegepast. Deze inbraaksigaleringsystemen hebben in het beveiligingsplan de functie een poging tot inbraak zo snel mogelijk waar te nemen en dit door te geven aan een partij die daarna zo snel mogelijk handelend op kan treden. Zoals in hoofdstuk 4 Beveiligingsplan van deel 3 is uiteengezet, dient het alarmsysteem bij voorkeur zo geprojecteerd te worden dat na detectie van het begin van een inbraak het forceren

van de fysieke beveiliging nog zoveel tijd vergt, dat de reagerende partij nog een redelijke kans maakt de inbreker(s) te pakken.

Deze (PIVA-AIRE-)filosofie wordt helaas nog steeds niet of onvoldoende toegepast bij de projectering van alarmsystemen, hetgeen in de praktijk inhoudt dat de hulpbiedende partij vaak alleen maar kan constateren dat er een inbraak heeft plaatsgevonden.

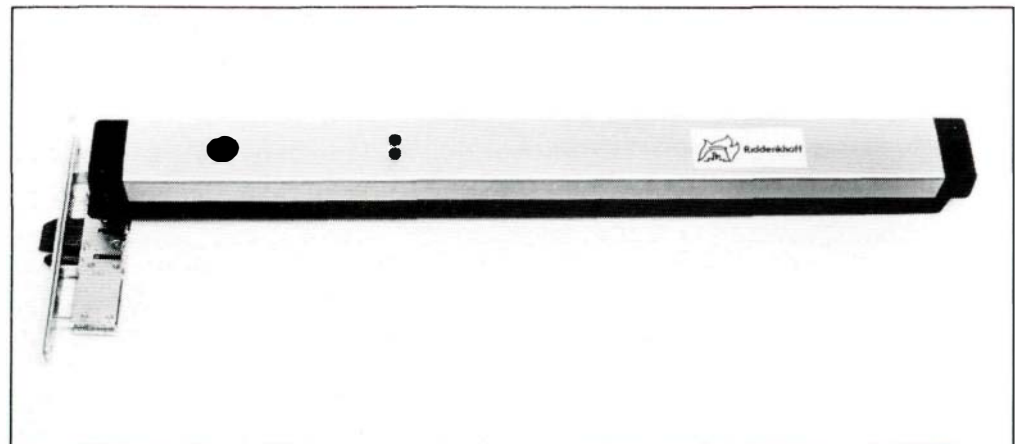
Werking

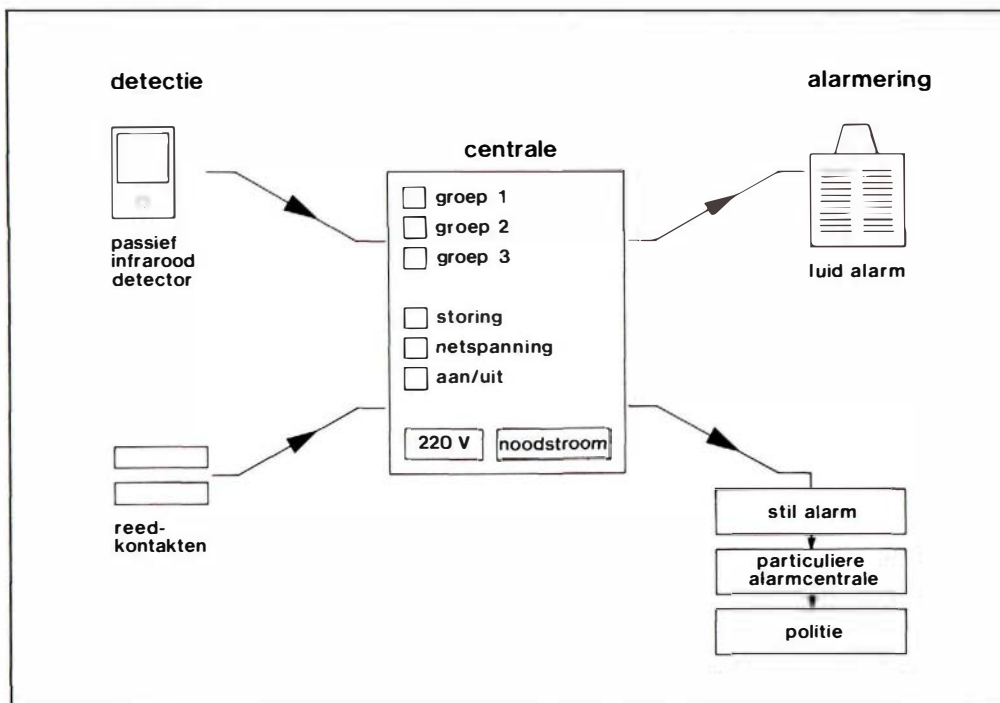
Alle alarmsystemen werken in principe gelijk. Een detector registreert een inbraak of een poging daartoe. Deze registratie wordt omgezet in een elektrische impuls, die naar de (veelal in de meterkast geplaatste) centrale van het systeem wordt gevoerd. Deze centrale zet de ontvangen impuls om in een alarmsignaal, dat met behulp van een automatische telefoonkiezer naar een particuliere alarmcentrale (PAC)* wordt verzonden. Deze PAC weet wat er na een dergelijke inbraakmelding gedaan moet worden en verwittigt bijvoorbeeld direct de politie en daarna de eigenaar of een meldadres en/of geeft opdracht aan een bewakingsdienst (ND)* zich naar de plaats van de inbraak te spoeden.

Naast of in plaats van het door de automatische telefoonkiezer verzonden alarmsignaal, kan gelijktijdig of vertraagd ook nog een optisch en/of akoestisch alarm in of nabij het kantoor worden ingeschakeld

Elektrisch bedienbare anti-panieksluiting

* = Particuliere alarmcentrale (PAC) en bewakingsdiensten (ND) vallen in Nederland onder het wettelijk toezicht van de overheid. Ze hebben derhalve een toelatingsnummer; zo spreekt men van PAC 12 en ND 143.





Schematische opbouw van een alarmsysteem

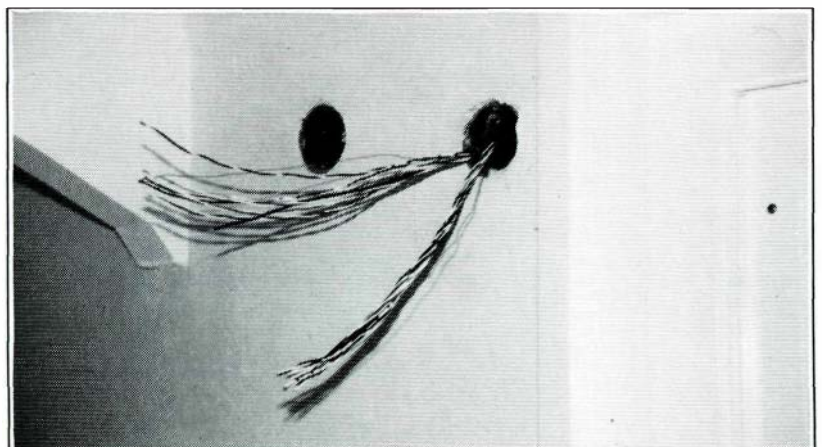
(bijvoorbeeld een flitslicht met sirene). Gezien het teruglopend effect van deze wijze van alarmering en de beperkende lokale verordeningen op het gebruik ervan, wordt deze laatstgenoemde wijze van alarmering steeds minder toegepast. Een overhaast vertrek van de inbreker(s) blijkt soms te kunnen worden bevorderd door één of meerdere flitslichten *in* het kantoor toe te passen die meteen na de detectie van de inbraak in werking treden. Daarna kan eventueel enkele minuten later nog een elektronische sirene *in* het kantoor in werking treden.

Installatie

Alarmsystemen zoals hier bedoeld, dienen bij voorkeur door erkende beveiligingsinstallateurs (UNETO-) te worden ontworpen, geleverd, geïnstalleerd en onderhouden. In de praktijk wordt vooral bij grotere projecten de bekabeling vaak aangelegd door de elektro-installateur die op het werk ook het merendeel van de overige elektro-installaties verzorgt. De beveiligingsinstallateur monteert dan de detectoren, de centrale enz., en levert het gehele inbraakdetectiesysteem op.

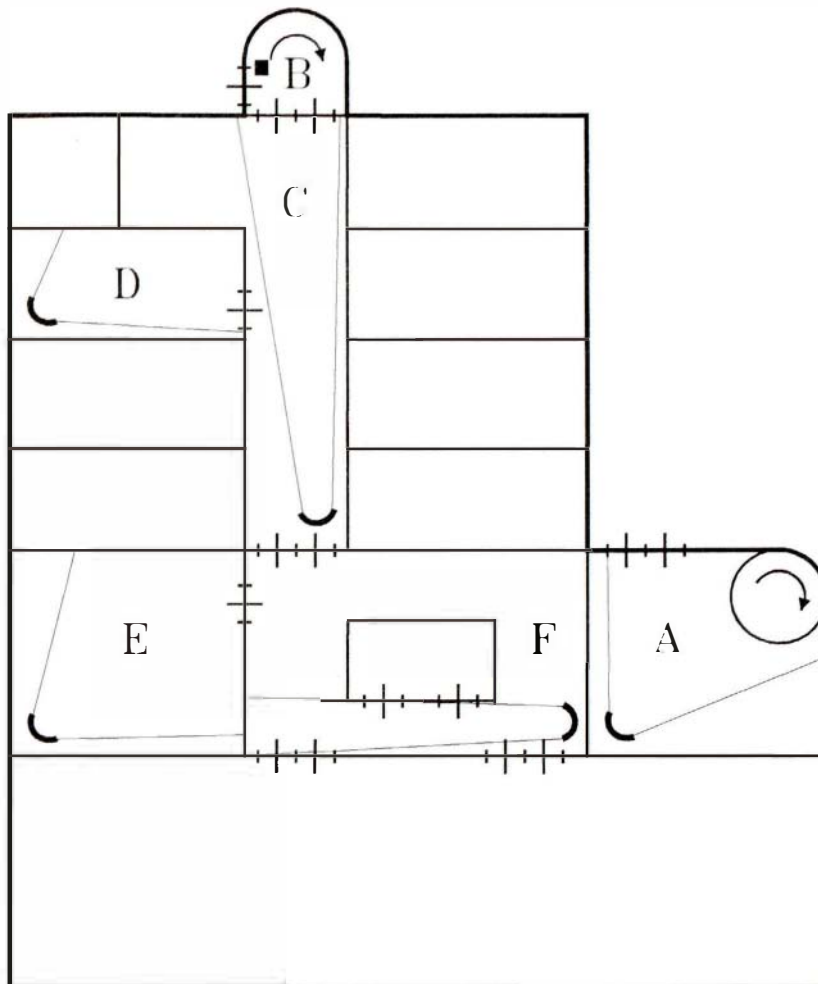
Met de Regeling voor de erkenning van elektronische beveiligingsinstallateurs, de zogenaamde REB 1983, worden onder meer het vakmanschap van de installateur en zijn 'planmatige aanpak' in het ontwerp van een beveiligingsplan beheerd. Het is dus een erkenning van diensten. De keuze van de componenten en de kwaliteitsbeoordeling daarvan is vooreerst nog aan de installateur. In de nabije toekomst hoopt men net als in een groot aantal andere landen ook tot een keurmerk op de componenten te komen.

Kabels worden soms door anderen getrokken; de beveiligingsinstallateur doet de rest



Plafond inbraakdetector**De bouwkundig ontwerper**

Voor de bouwkundig ontwerper is het raadzaam al vanaf het begin van het bouwproces aandacht te hebben voor het onderwerp elektronische beveiliging. In een later ontwerpstadium kunnen dan het bouwkundige en het elektronische deel van het beveiligingsplan op elkaar worden afgestemd. Op die manier kunnen bijvoorbeeld ook tijdig de eventuele esthetische bezwaren van bepaalde in het zicht komende detectoren worden ondervangen, kunnen voldoende (loze) leidingen voor het alarmsysteem worden gereserveerd en kan de installateur eindelijk eens *voldoende ruimte* in de meterkast of andere gelijksoortige ruimten aantreffen om de noodzakelijke componenten te installeren en later te kunnen onderhouden.

*Typische inbraak-
detectie-projectering*

Voorbeeld van een inbraakdetectie-projectering op de begane grond van een kantoor met een 'gemiddeld' inbraakrisico

- A = hal met entree en trappenhuis, ruimtelijk beveiligd
- B = vluchtdoor in noodtrappenhuis, magneetcontact
- C = gang, ruimtelijk beveiligd
- D = ruimte met verhoogd risico, ruimtelijk beveiligd
- E = ruimte met verhoogd risico, ruimtelijk beveiligd
- F = ruimte voor deuren van liften en grote (onbeveiligde) kantoorruimte, ruimtelijk beveiligd

*Toegangscontrole in het
computergebied; in dit
geval met sleutelkaart
en sluis*



We kunnen een kantoorgebouw met inhoud in zijn geheel trachten te beschermen tegen dreigende criminaliteitsrisico's. Die risico's blijken in het kantoorgebouw evenwel niet zo vaak gelijkmatig te zijn verspreid, zodat het zinvol is de zeer risicovolle plekken te isoleren van de rest en ze afzonderlijk een hogere graad van beveiliging mee te geven. Men duidt deze benadering vaak aan met de term 'compartimenteren'. Dat is een reeds lang bestaande benadering want al sinds mensenheugenis brengt men in kantoren bijvoorbeeld geld in een kluisruimte onder of dossiers in speciale voor dit doel gebouwde archiefruimten.

We zullen in dit hoofdstuk trachten de ontwerper zoveel mogelijk achtergrondinformatie te geven van een aantal zeer belangrijke compartimenten in kantoorgebouwen. Dit zal duidelijk maken dat het in het algemeen gewenst is dat de ontwerper in een zo vroeg mogelijk stadium een specialist in het ontwerp moet betrekken

We behandelen achtereenvolgens:

- *Computerruimten;*
- *Archiefruimten:*

de traditionele ruimten voor veel dossiers met papier, alswel de steeds meer in opkomst zijnde archiefruimten voor magnetische informatiedragers.

- *Kluisruimten:*

de min of meer traditionele — zeer sterke — inbraak- en brandwerende kluisruimten.

- *Brand- en inbraakwerende kasten:*

de 'losse eenheden' die afhankelijk van hun constructie zijn bedoeld voor:

- brand- en inbraakwering;
- brandwering (algemeen);
- brandwering (specifiek voor magnetische informatiedragers; 'data-safes').

- *Ruimten voor geldzaken:*

ruimten waarin bijvoorbeeld het geld wordt geteld.

- *Bewakingsruimten:*

ruimten met een specifieke functie binnen de beveiliging van het gebouw.

Het criminele risico rond het compartiment kan vrijwel nooit los worden gezien van het brandrisico. Dat onderwerp wordt in dit rapport in principe niet behandeld (hierover is voldoende goede literatuur* voorhanden), maar waar nodig (zoals bij data-kluisen) wordt er zo hier en daar wel op brandzaken ingegaan.

COMPUTERRUIMTEN

We denken hierbij aan een 'doorsnee' computerruimte in een kantoorgebouw. Ruimten met personal computers en/of werkstations worden hier dus niet bedoeld. Het ontwerp voor computerruimten is zeer zeker bij grotere computers (soms is het gebouw 'meer computer dan kantoor') een specialisme van de computerfabrikant. Het verdient derhalve aanbeveling deze fabrikant reeds in een zo vroeg mogelijk stadium in het ontwerp te betrekken.

De computerruimte zoals hier bedoeld kunnen we in het algemeen onderverdelen in ruimten voor bijvoorbeeld:

- operateurs;
- klimaatregeling;
- automatische brandblusinstallatie;
- opslag materiaal;
- systeembeheerder;
- secundaire opslag informatiedragers.

Deze ruimten dienen als één geheel gecompartmenteerd te zijn van de rest van het kantoorgebouw.

Wanneer de definitieve plaats voor de computerruimte nog niet is bepaald, is het goed om te bedenken dat er nogal wat wensen voor het ontwerp van de lokatie bij de computerspecialisten liggen.

* = Bijvoorbeeld:
'Een brandveilig gebouw ontwerpen', uitgave: Stichting Bouwresearch
Bouwresearch
(SBR-publicatie 91)

Vrij vertaald komen ze erop neer dat de computerruimte gemakkelijk maar tevens goed controleerbaar bereikbaar moet zijn, en zo min mogelijk aan invloeden van buitenaf onderhevig moet zijn (bijvoorbeeld geen hinderlijk zonlicht of productie- en/of verkeerslawaaï), kortom een soort 'oase' in het kantoorgedruis. De voorkeur gaat uit naar computerruimten in één horizontaal vlak. Een uitbreiding naar een verdieping hoger of lager is dus niet gewenst. Met het reserveren van ruimte voor uitbreiding zal dus met dit aspect rekening moeten worden gehouden.

De specifieke onderwerpen zoals: computervloeren, klimaatregeling, verlichting, vloer- en wandbedekkingen, noodstroomvoorziening, geluidsniveau, overspanning, bekabeling enz., laten we over aan de specialisten en we kijken nu wat er resteert aan specifieke aandachtspunten voor de veiligheid en beveiliging.

Risico's en ligging

In eerste instantie zal de opdrachtgever of diens risk-manager moeten aangeven hoe hoog de risico's worden ingeschat, zodat de mate van beveiliging en de uitvoering daarvan kan worden bepaald (zie hier ook hoofdstuk 5: het RRIM). Tegen geplande criminele acties kunnen we ons met bouwkundige, elektronische en organisatorische middelen weerbaar maken. Bij risico's als overstroming, explosie (belendende industrie), verkeer (voer-, vaar- en vliegtuigen) blijkt soms te moeten worden overwogen het gebouw maar elders neer te zetten. Wanneer de concentratie aan computers in één kantoor te groot wordt, kan worden overwogen dit risico te spreiden over meerdere vestigingen.

Het gebouw

Computerapparatuur met toebehoren en daarbij behorend personeel moeten in een afzonderlijke ruimte met toegangscontrole worden ondergebracht. Alhoewel vanuit beveiligingsoogpunt een centrale ligging zonder aansluitende bui-

tengevels in het kantoorgebouw wenselijk is, moet er wel gedacht worden aan wetgeving op het gebied van arbeidsomstandigheden en de wens van het personeel naar buiten te kunnen kijken. Wanneer glas in de buitenschil van de computerruimte wordt toegepast, moet dit worden afgestemd op eerder genoemd risiconiveau. Dat kan derhalve variëren van 'licht slagwerend tot slag- en kogelwerend' (zie hoofdstuk 7). Er moeten bij voorkeur geen parkeergarages en ruimten met een hoge vuurbelasting onder computerruimten worden geprojecteerd.

Het verdient aanbeveling computerruimten eerder op hoger gelegen verdiepingen te projecteren dan op de begane grond. De buitengevels moeten inbraakwerend zijn en moeilijk te beklimmen. Speciale aandacht verdienen hierbij de vluchtwegen (zie hoofdstuk 7), een eventueel plat dak met lichtdoorlatende openingen, rookluiken en dergelijke. Inlaatopeningen voor verse lucht moeten bestand zijn tegen inbraak en rook- of gasaanvallen.

Toegangscontrole

Het computerruimtegebied dient door een toegangscontrolesysteem te worden beschermd tegen ongewenste bezoekers. Maatregelen die de bewegingen van het personeel en de materialenstroom controleerbaar maken zijn onder meer het toepassen van:

- één entreepartij;
- een toegangscontrolesysteem (wordt uitvoerig behandeld in de hoofdstukken 9 en 10);
- sloten met tijdregistratie op van belang zijnde deuren;
- garderobe- en toiletruimten in het door het toegangscontrolesysteem beveiligde gebied;
- een opslag voor papier en dergelijke (dagvoorraad), eveneens in het beveiligde gebied;
- binnenwanden met slagwerend glas;
- een eventueel persoonsgebonden toegangscontrole voor data-archief ruimten.

Data-archiefruimten

Duplicaat-informatiedragers moeten in een data-archiefruimte worden opgeslagen en fysiek worden gescheiden van de operationele archieven, zodat bij een ramp op z'n minst één archief intact blijft. De constructie van dit soort ruimten wordt behandeld in in een volgende paragraaf. In het algemeen moeten in dit soort ruimten worden toegepast:

- wanden en deuren met een brandwerendheid van 1,5 uur;
- cilindersloten met sleutelcertificaat, alleen van buitenaf te bedienen;
- Een telefoon;
- een brand- en inbraakdetectiesysteem;
- een minimale vuurbelasting in aangrenzende ruimten;
- het vermijden van opslag langs buitengevels;
- brandpreventieve voorzieningen in het luchtbehandelingssysteem;
- automatisch werkend blusgassysteem (Halon 1301).

ARCHIEFRUIMTEN

Het verdwijnen van gegevens op papier, microfilm of magnetische informatiedragers kan voor een bedrijf rampzalig zijn. Naast diefstal en inbraak kan dit ook worden veroorzaakt door brand of brandstichting. Het is dus duidelijk dat gegevens goed moeten worden beschermd en al lange tijd plegen wij dat met behulp van archiefruimten te doen. Jammer is dat de goed ogende archiefruimten vaak maar een zeer beperkte bescherming bieden, vooral wanneer de gegevens niet meer op papier staan.

We kunnen onderscheid maken in de traditionele archiefruimten voor papieren zaken zoals boeken, rapporten, dossiers enz. en die welke volledig zijn toegesneden op de magnetische informatiedragers; de 'datakluizen'. Deze laatste moeten we niet verwarren met de kluizen die onder Kluisruimten in dit hoofdstuk worden behandeld. Dat zijn de min of meer

traditionele — zeer sterke — inbraak- en brandwerende kluizen.

Traditionele archiefruimten

Deze ruimten moeten brand- en inbraakwerend worden uitgevoerd. Een goede referentie voor de uitvoering van dit soort ruimten is het Voorschrift inrichtingseisen voor nieuwe archiefruimten in Nederland, zoals gepubliceerd in de Nederlandse Staatscourant van 6 september 1983.

Hierin worden eisen genoemd met betrekking tot:

- ligging van een gebouw;
- bouwkundige voorzieningen;
- brandbeveiliging;
- klimaatbeheersing.

Het voorschrift behandelt niet de inbraakwerendheid. Deze dient te worden uitgevoerd met de uitgangspunten zoals deze in hoofdstuk 7 van dit rapport aan de orde komen.

Een bruikbare referentie voor ontwerpers van archiefruimten is voorts hoofdstuk 5000 Archiefbeheer/bouwzaken uit het Handboek archiefbeheer in de praktijk (Samson).

Zeker bij overheidskantoren, maar ook bij niet-overheidsprojecten kan door opdrachtgevers of ontwerpers advies worden ingewonnen bij de Provinciale Archiefinspecteur, in het Provinciehuis van de betreffende provincie gevestigd.

Voorts is er nog een Landelijk Overleg Provinciale Archiefruimten (Postbus 122, 9400 AC Assen) waar nadere informatie kan worden ingewonnen.

Duitsland kent een norm voor de bouw van archiefruimten, de DIN 4102: Empfehlungen für den Bau von Archivräumen kunnen gratis worden aangevraagd bij het Forschungs- und Prüfgemeinschaft Geldschränke und Tresoranlagen e.V., Postfach 710864, D- 6000 Frankfurt 71.

Data-archieven

Papier kan de gevolgen van een brand relatief goed doorstaan. Magnetische informatiedragers zijn echter zo gevoelig voor temperatuurstijgingen en verhogin-

De zeer belangrijke keurmerkplaatjes voor brandkasten, data-safes, data-archiefruimten, kluisdeuren, enz.

DATENSICHERUNGSRaum	
Prüfvermerk	
Güteklasse	R 60 D
Fabr. Nr.	
Baujahr	
Typgepr. nach	RAL-RG 626/B
durch Forschungs- und Prüfgemeinschaft Geldschranke u. Tresoranlagen e.V. Frankfurt	

STAHLsCHRANK	
Prüfvermerk	
Sicherheitsstufe	C 2
Fabr. Nr.	
Gewicht	
Baujahr	
Typgepr. nach	RAL-RG 626/2
durch Forschungs- und Prüfgemeinschaft Geldschranke u. Tresoranlagen e.V. Frankfurt	

TRESORTÜR	
Prüfvermerk	
Sicherheitsstufe	T 10 KB EX
Fabr. Nr.	
Gewicht	
Baujahr	
Typgepr. nach	RAL-RG 623/10
durch Forschungs- und Prüfgemeinschaft Geldschranke u. Tresoranlagen e.V. Frankfurt	

DATENSICHERUNGSSCHRANK	
Prüfvermerk	50143
Güteklasse	S 60 DIS
Fabr. Nr.	
Leergewicht	
Baujahr	
Typgepr. nach	RAL-RG 626/7
durch die Forschungs- und Prüfgemeinschaft Geldschranke u. Tresoranlagen e.V. Frankfurt	

PANZER - GELDSCHRANK	
Prüfvermerk	
Sicherheitsstufe	D10
Fabr. Nr.	
Gewicht	
Baujahr	
Typgepr. nach	RAL-RG 626/10
durch die Forschungs- und Prüfgemeinschaft Geldschranke u. Tresoranlagen e.V. Frankfurt	

gen van de relatieve vochtigheidsgraad, dat de gevolgen dramatisch kunnen zijn. Eenvoudige, kleine computers en geringe databestanden zijn goed te beschermen met speciale datakasten. Daarvan zijn er nogal wat te koop en ze voldoen doorgaans goed wanneer ze voldoen aan de VDMA-normen; we behandelen deze producten in een volgende paragraaf van dit hoofdstuk. Grotere concentraties databestanden dienen te worden opgeborgen in daarvoor bestemde kluisruimten die eveneens aan de VDMA-normen moeten voldoen.

VDMA-normen

Er zijn diverse instituten die datakasten ('datasafes') en/of data-archiefruimten testen, zoals bijvoorbeeld UL (Underwriters Laboratories, Chicago USA), maar voor het merendeel hebben we met dit onderwerp in Europa te maken met de normen van de VDMA (Verband Deutscher Maschinen- und Anlagenbau e.V. te Frankfurt).

De belangrijkste normen zijn:

VDMA 24990:

- Geldschranke und Tresoranlagen, Begriffe.

VDMA 24991:

- Teil 1, Prüfbedingungen für das Brandverhalten von Stahlschränken und sonstigen Behältern;
- Teil 2, Prüfbedingungen für das Brandverhalten von Räumen zur Aufbewahrung von Datenträgern.

VDMA 24992:

- Stahlschränke der Sicherheitsstufen A und B, Begriffe und Mindestanforderungen.

De VDMA-norm 24991, deel 2, heeft dus betrekking op de databescherming tegen brand, en de VDMA 24992 tegen inbraak. Wanneer een product op dit gebied getest is volgens de VDMA en is goedgekeurd, mag het een RAL-keurmerk dragen van het Deutsches Institut für Gütesicherung und Kennzeichnung e.V. en dat zien we dan weer op het merkplaatje van een product staan. Zo is bijvoorbeeld: Typegepr.

Aanduiding	Begintemperatuur in kast of kluis	Max. temperatuur verhoging in kast	Max. luchtvochtig heid in kast of kluis
P (Papier)	+ 20° C +/- 5° C	+ 150 K	—
D (Datentrager)	+ 20° C +/- 5° C	+ 50 K	85%
DIS (Disketten)	+ 20° C +/- 5° C	+ 150 K	85%

Temperatuurstijgingen in drie klassen

nach RAL-RG 626/7, een volgens VDMA 24991, deel 2: Type-goedgekeurde datasafe. Vermeld het merkpiaatje: Typegepr. nach RAL-RG 626/8, dan betreft het een datakluis.

Datakluizen

Men beschermt magnetische informatiedragers niet in betonnen kluizen met wanden van 200 mm of dikker. Vocht uit het beton zal bij brand als waterdamp in de kluis terechtkomen. De relatieve vochtigheid loopt daardoor op tot boven de 85%, de fatale grenswaarde voor magnetische informatiedragers. Ook archiefruimten gebouwd volgens DIN 4102 zullen niet voldoen. Bij deze norm wordt de luchtvochtigheid in de ruimte niet gemeten, en er valt dus niet te garanderen dat deze onder de 85% blijft.

Data-kluizen (en kasten) moeten, zoals eerder vermeld, voldoen aan VDMA 24991. De eisen en beproevingsmethoden van deze norm gaan vrij ver, hetgeen mag blijken uit het volgende:

- Datakasten en -kluizen worden minstens één uur en maximaal twee uur

verhit tot 1000° C, waarna een natuurlijke afkoeling (in de oven) volgt.

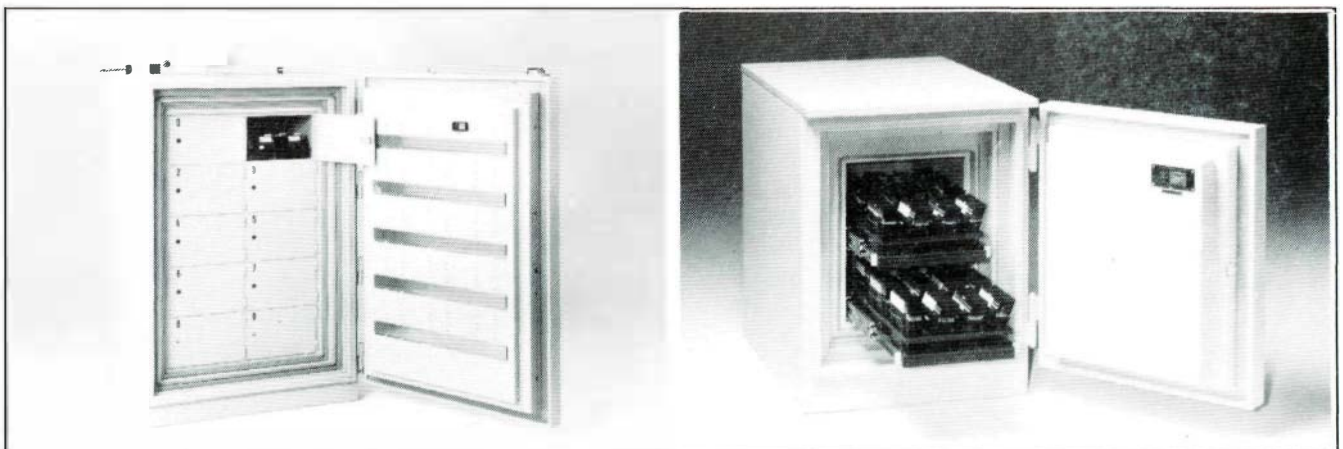
- Ze worden blootgesteld aan plotselinge extreme temperatuurverschillen.
- Ze moeten de eigenschap van 'de kooi van Faraday' hebben en extreme magnetische invloeden kunnen weerstaan.
- Tijdens en na de test mag de temperatuur binnen bepaalde grenzen stijgen, terwijl de relatieve vochtigheid niet meer mag bedragen dan 85%.

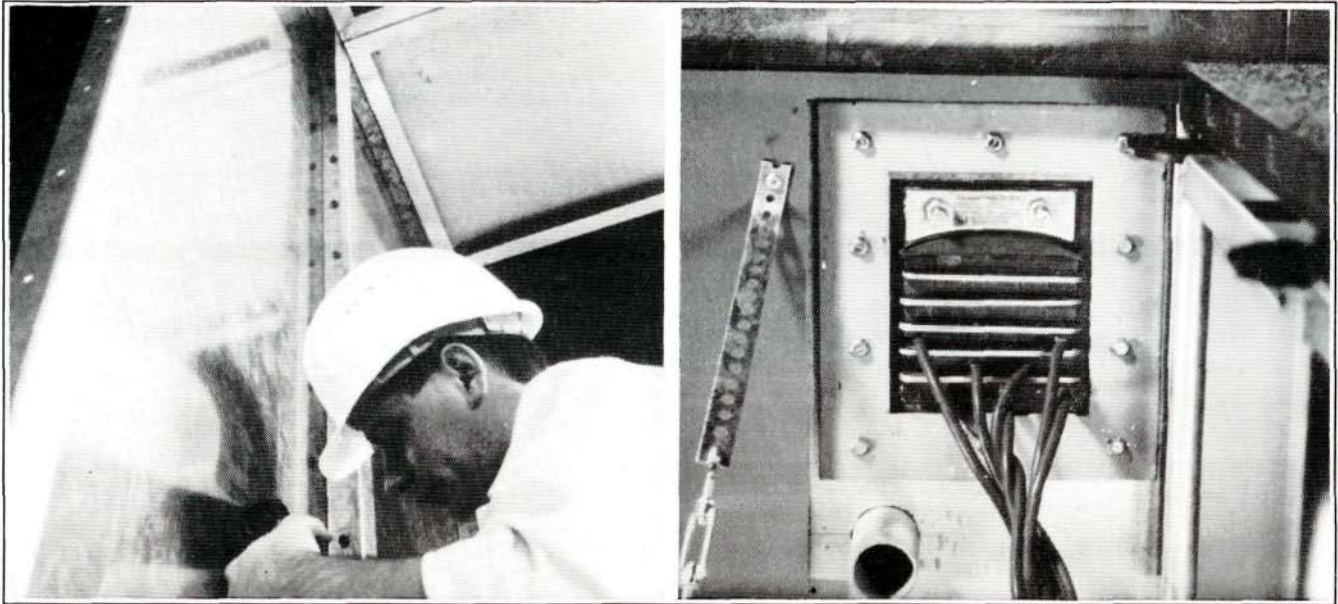
Voor de 'vuurbelasting' in de oven kent men in de betreffende VDMA-norm twee klassen, 60 of 120 minuten in de vlammen. Men geeft dit aantal minuten ook in de klassering aan, men spreekt van een S 60 of S 120-kast (de S staat voor Schrank), of bij kluizen voor een R 60 of R 120-kluis (R staat voor Raum).

Voorts kent men voor het meten van de temperatuurstijgingen nog eens drie klassen welke in bovenstaande tabel staan vermeld.

Hebben we dus een RAL-RG 628/8 type-goedgekeurde kluis met een klassering R 60 DIS, dan weten we dat deze kluis (R) op basis van de VDMA 24991 deel 2 is getest,

*'Data-safes':
Specifieke brandwering
voor magnetische
informatiedragers
Let op de keurmerkplaatjes aan de binnenzijde
van de deur.*





Datakluis

links:

Het bouwen van de stalen binnencel

rechts:

Detail van de kabeldoorvoer

60 minuten met vuur is belast, waarbij uiteindelijk de luchtvochtigheid in de kluis de 85% niet heeft overschreden, en de temperatuurverhoging niet meer dan 30 K is geweest (DIS). De Duitsers hebben met de VDMA-normen en bijbehorende klasseringen de datakasten en kluizen goed 'im Griff', en dat is maar goed ook, want er zijn nogal wat misverstanden op dit gebied, hetgeen de bekende misleidingen in de markt van de leveranciers tot gevolg heeft.

Hoe bouwt men nu deze kluizen?

Er zijn twee benaderingen: Het bouwen van een geheel nieuwe datakluis, of het verbouwen van een bestaande brandwerende archiefruimte tot een datakluis. Bij een verbouwing van een bestaande archiefruimte moet deze wel voldoen aan de klassificatie F 90 volgens DIN 4102.

In deze ruimte bouwt men met stalen elementen een binnencel. Deze cel is geheel vrijstaand. In dit systeem zijn alle vereiste openingsafsluitingen voor de binnen- en buitencel opgenomen.

De wand-, plafond- en vloerelementen van de binnencel zijn dubbelschalige gesloten constructies met een speciale isolatie. Staalprofielen in de constructie zorgen voor versteviging en garanderen de eigen stabiliteit en elasticiteit tegen me-

chanische en thermische invloeden. De afzonderlijke elementen worden eenvoudig in elkaar gelast en vormen zo een binnencel. Keramische en duurzaam-elastische afdichtingen, gecombineerd met extra opgelaste stalen profielen op alle elementverbindingen, voorkomen dat vocht en rookgassen kunnen binnendringen. De binnenwanden worden met bijvoorbeeld een onbrandbaar glasweefsel afgewerkt. Het gewicht van de binnencel-elementen bedraagt in afgewerkte situatie circa 55 kg/m². De vloerelementen zijn te belasten met maximaal 1.600 kg/m². In alle elementen van de binnencel mag niet geboord of geschroefd worden.

Bij complete nieuwbouw wordt voorts een buitencel gebouwd, eveneens van verzinkte staalplaat-elementen met een hitte-isolerende vulling. Ook deze zijn verstevigd met staalprofielen en worden ter plaatse afgedicht en aan elkaar gelast. De elementen van de buitencel wegen afgewerkt circa 45 kg/m². De totale constructie van buitencel – spouw – binnencel is circa 200 mm (wand)dikte.

Naast de celconstructie hebben dergelijke kluizen nog een aantal andere onderdelen. Dat zijn de brandveilige kluisdeurinstallatie, luiken voor luchtbehandeling, kabeldoorvoersystemen, een lichtinstallatie met schakelkast, telefoon, noodver-



boven en
onder:
Data-kluisruimten

lichting en vloerbedekking. Alle installaties en voorzieningen worden door in dit vak gespecialiseerde kluizenbouwers verricht. Pas buiten de kluiswanden mogen derden verdere aansluitingen verzorgen. De kluis kan tegen brand in de kluis beveiligd worden door een blusgasinstallatie (Halon 1301).

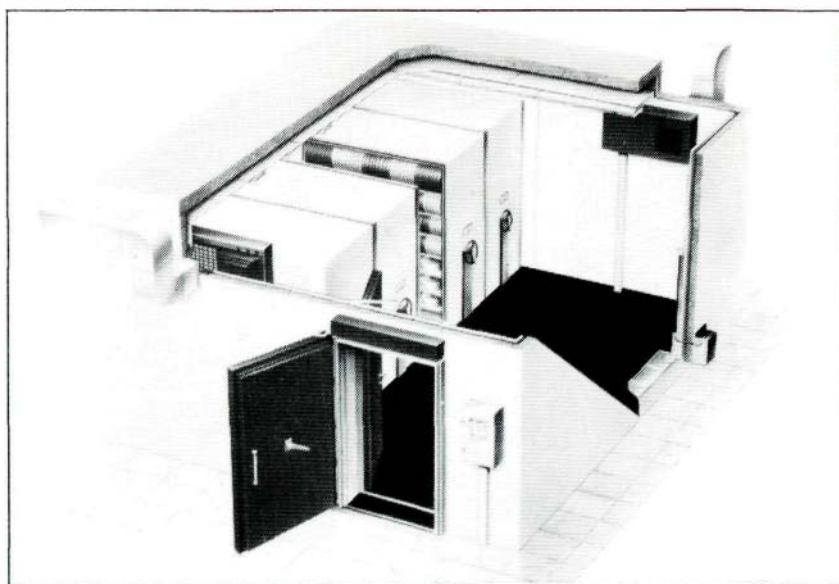
Datakluizen, in constructies zoals hiervoor geschetst, beschermen de inhoud tegen brand, rook, water(damp), in- en uitstraling van hoogfrequent-signalen, magnetische stralen en zijn verder explosie- en inbraakwerend.

KLUISRUIMTEN

Indien de op te bergen waarden zeer groot zijn en/of de inhoud van een brandkast te boven gaan, worden kluizen toegepast. Hieruit volgt dat de weerstand van een kluis tegen 'crimineel geweld' als regel groter moet zijn dan van een brandkast. Kluizen hebben de functie de erin geborgen waarden te beschermen tegen brand of tegen brand en inbraak. Ruimten die bescherming mochten bieden tegen oorlogsgeweld vallen hier dus buiten, evenals de kluisruimten die speciaal bedoeld zijn voor de bescherming van magnetische informatiedragers: de datakluizen. Deze

werden behandeld in de vorige paragraaf. In het algemeen kunnen kluizen die uitsluitend tegen brand bescherming moeten bieden (zoals bijvoorbeeld archiefkluizen) van een eenvoudiger constructie zijn dan kluizen die tegen brand en inbraak bescherming moeten bieden.

We zullen de eerste categorie gemakshalve maar *archiefkluizen* noemen, en de tweede categorie de *brand- en inbraakwerende kluizen*. In deze paragraaf zullen we ons uitsluitend bezighouden met de voor-



waarden waaraan de laatstgenoemde categorie moet voldoen.

Eisen voor de gehele kluis

De eisen waaraan een kluis in zijn geheel moet voldoen kunnen als volgt worden omschreven:

1 De sterkte die aan een kluis gegeven moet worden, hangt af van de waarden die erin geborgen zullen worden. In vrijwel alle gevallen zal de kluiswanddikte, die nodig is om een bepaalde inbraakwerendheid te verkrijgen, ruim voldoende brandwerendheid bezitten. Anders is het gesteld met de sterkte van de kluis in zijn geheel, vandaar punt 2.

2 De kluis zal zo in een gebouw moeten zijn gesitueerd, dat hij een eventuele brand kan doorstaan.

De maatregelen die daarvoor moeten worden getroffen, zullen onder andere afhangen van de plaats van de kluis (een kluis in een kelder vraagt een andere ondersteuning dan een kluis op bijvoorbeeld een vijfde verdieping).

3 De kluis moet aan alle zijden (wanden, vloer, plafond) even sterk zijn. Uiteraard kunnen er zich omstandigheden voordoen, die een plaatselijke versterking om andere dan inbraaktechnische redenen noodzakelijk maken.

4 De plaats van de kluis moet zo worden gekozen, dat zich in de onmiddellijke omgeving geen muren, spanten (naast of boven de kluis) en dergelijke bevinden, die zo sterk zijn, dat ze tot steun voor inbrekerswerktuigen kunnen dienen, bijvoorbeeld bij gebruik van vijzels of 'porta-powers'.

5 De wanden, de vloer en het plafond van een kluis mogen door een eventuele inbreker niet ongezien benaderd kunnen worden. Dit houdt bijvoorbeeld in dat een kluiswand, grenzend aan een ander perceel, voorzien moet worden van een controlegang en dat onder de vloer van een kelderkluis een controleruimte moet zijn. Staat de kluis in het grondwater, dan worden door dat feit aanvalspogingen van buiten het gebouw in grote mate bemoeilijkt; in dat geval zal de controleruimte

onder de kluisvloer minder noodzakelijk zijn.

6 De buitenste muur van de controlegang mag niet als steun voor inbraakwerktuigen kunnen worden gebruikt, dit kan worden bereikt door:

- te zorgen dat deze muur veel minder sterk is;
- erop te letten, dat zich achter deze muur geen andere muren bevinden die de controlegang sterkte kunnen geven;
- de ruimte in de controlegang tussen de beide muren zo klein mogelijk te houden, zodat er moeilijk apparatuur geplaatst kan worden en de aanvaller/inbreker vrijwel geen bewegingsmogelijkheid heeft.

7 Bij de keuze van de plaats van de kluis moet in het oog worden gehouden dat het in de toekomst noodzakelijk kan zijn de kluisdeur uit de wand te breken om deze af te voeren. Deze situatie kan zich bijvoorbeeld voordoen wanneer de deur gedurende een inbraakpoging ernstig is beschadigd. Wanneer de kluisvloer onder het grondwaterpeil ligt, moeten ter plaatse van de dorpel reeds bij de bouw extra maatregelen worden getroffen tegen lekkage bij een eventueel uitbreken van de deur.

8 Het leggen van afvoerbuizen, airconditioningskanalen, verwarmingsbuizen en dergelijke door de kluiswand heen moet ten sterkste worden ontraden! Al deze doorboringen betekenen een verzwakking van de kluis.

9 Op dezelfde gronden moet het aanbrengen van ventilatiekokers worden afgeraden; wil men de kluis ventileren, dan kan dit door toepassing van een nood- of mangatdeur of een tweede even grote en even sterke kluisdeur, uiteraard met gebruikmaking van ventilatiehek(ken).

10 Om redenen genoemd in 8 kan als verwarmingsbron in de kluis geen gebruik worden gemaakt van heet water, hete lucht of gas. Wel kan elektrische verwarming gekozen worden. Ook kan via de kluisdeur(en) warme lucht in de kluis geblazen worden. Beide verwarmingssystemen zijn alleen overdag te gebruiken.

11 Bij het ontwerp van de kluis dient men te overwegen of er maatregelen getroffen moeten worden tegen het binnendringen van water, afkomstig van bluswater gebruikt bij een eventuele brand of van een overstroming.

12 Beveiliging van de kluis en zelfs de ruimte eromheen met goede alarmerings-apparatuur verdient sterke aanbeveling. Om een optimale beveiliging te verkrijgen dient vóór het ontwerp van de kluis contact te worden opgenomen met de fabrikant/leverancier van de kluisdeur.

13 Het verdient overweging in de kluis een telefoon aan te brengen; eventuele ingesloten krijgen daardoor de kans zich te laten bevrijden.

Eisen voor kluiswanden, vloer en plafond

Kluiswanden worden als regel gebouwd van een materiaal of een samenstelling van materialen, die bescherming moet bieden tegen inbraakpogingen en brand. Hoewel het in principe mogelijk is gemetselde kluizen te bouwen van harde klinkers, verdient het gebruik van beton aanbeveling. De voornaamste reden is dat het bijzonder moeilijk is een goede bewapening tegen inbraakpogingen in gemetselde muren aan te brengen.

Als tweede reden zou genoemd kunnen worden, dat de kwaliteit van beton meer in de hand gehouden en beter gecontroleerd kan worden dan van gemetselde muren.

We gaan er hier dan ook vanuit dat beton als hoofdbestanddeel wordt gebruikt.

1 Eisen te stellen aan het beton:

40 cm. gewapend beton, kwaliteit B 37,5 klasse II (gemeten volgens de VB 1974). Verwerkbaarheid betonspecie: maximale consistentiegebied: 3.

2 Eisen te stellen aan de toeslagmaterialen:

De WCF (water-cement-factor) mag nimmer hoger zijn dan 0,5. Nominale korrel van het grind: 31,5. Cement in de klasse B of C mag gebruikt worden, evenals bepaalde toeslagmiddelen, zoals bijvoorbeeld (super) plastificeerders (chloride-vrij).

De betonmortelcentrale, die het beton levert voor de kluis, dient goedgekeurd te zijn door de Betonvereniging. Bij het storten van het beton dienen kisttrillers ('Wacker'-trillers) in combinatie met trilnaalden te worden gebruikt. Hierbij dient rekening te worden gehouden met stalen bekisting.

3 Eisen te stellen aan de bewapening:

Als anti-inbraakbewapening, dienen twee kruisnetten van een staalsoort FEB 400–FEB 500 met een doorsnede van 16–18 mm en een maaswijdte van ± 15 cm ten opzichte van elkaar verspringend te worden opgenomen. Als vervanging van de kruisnetten kan ook speciaal daartoe door de leveranciers van veiligheidswerken vervaardigd, getordeerd staal worden toegepast (voor toepassing en verwerking wordt verwezen naar de instructies van de leverancier).

4 Aanstorten van deuren:

Wat geldt voor het storten van wanden, plafonds en vloerplaten, geldt in nog sterkere mate voor het aanstorten van gestelde deuren, namelijk de uiterste zorg om grindnesten te voorkomen en geen gebruikmaking van een dunne specie of zogenaamde 'zwelspecie'. Ook het rond het kozijn aan te storten beton moet van een uitstekende kwaliteit zijn.

Veiligheidsmaatregelen tijdens de bouw

In de regel realiseert men zich te weinig, dat tijdens het bouwen van een kluis door lieden, die ver in hun duistere toekomst vooruit denken, voorbereidingen getroffen kunnen worden die een illegale toegang tot de kluis op een later tijdstip mogelijk maken. Bijvoorbeeld door op sommige plaatsen gebruik te maken van ondegdelijk beton of het gedeeltelijk wegnemen van goed, pas gestort beton om dat te vervangen door goed gecamoufleerd, gemakkelijk wegneembaar materiaal. Scherpe controle bij het maken van de kluis is dan ook vereist. Dit geldt zowel voor het aanbrengen van de bewapeningnetten als voor het mengen en storten van het beton.

Prefabkluizen zijn voor wat betreft dit

soort risico's in het voordeel.

Ook het bewerken van de ter plaatse opgestelde kluisdeur(en) behoort tot de mogelijkheden. Als de achterzijde van de kluisdeur (met het slotwerk enz.) voor iedereen toegankelijk is, kunnen overdag, 's nachts of gedurende de weekeinden, vele soorten sabotagedaden gepleegd worden.

Het is daarom noodzakelijk dat, naast de door de fabrikant uitgevoerde controle van de kluisdeur tijdens de afmontage direct voor de overdracht, het werkterrein zowel overdag als 's nachts nauwlettend wordt bewaakt en de werkzaamheden aan de kluis zorgvuldig worden gecontroleerd.

BRAND- EN INBRAAKWERENDE KASTEN

Brand- en inbraakwerende kasten behoren tot een zeer gespecialiseerd vakgebied waarbij het de ontwerper (en gebruiker) gemakkelijk wordt gemaakt door de 'Brandkastenlijst' van de Stichting Kwaliteitsbeoordeling Brandkasten en kluizen (SKB, zie onder Organisaties en instellingen). De teksten in deze paragraaf zijn dan ook ontleend aan publikaties van deze stichting.

Voor alle duidelijkheid moet worden gesteld dat het verzamelwoord brandkast nogal eens tot misvattingen leidt. Men onderscheidt in het algemeen de 'brandkasten' in:

- brand- en inbraakwerende kasten;
 - brandwerende kasten;
 - brandwerende kasten voor magnetische informatiedragers ('data-safes').

De SKB houdt zich — anders dan adviezen — niet direct bezig met de beoordeling van kluizen (archief- of datakluizen), maar wel met de beoordeling van kluisdeuren.

Voor genoemde 'Brandkastenlijst' heet eigenlijk 'Advies voor verzekering van geld in brandkasten en kluizen' hetgeen de oorsprong van de lijst zo'n beetje aangeeft. Wanneer bekend is hoeveel geld

doorgaans ongeveer moet worden opgeborgen, kan met de SKB-lijst de 'zwaarte' ofwel het type van één of meerdere van de circa 50 verschillende merken brandkasten worden bepaald. Deze benadering wordt in Nederland min of meer als norm gehanteerd, zeer zeker wanneer er geld moet worden verzekerd. Gaat het bijvoorbeeld om circa f 150.000,- aan contanten die moeten worden opgeborgen, dan zou volgens de SKB-lijst bijvoorbeeld een Chubb-Lips-kast type VS of een Martens-kast type TRA in aanmerking komen. Het gaat hierbij dan om een standaarduitvoering (bijvoorbeeld zonder tweede slot) van de brandkast, die geacht wordt in een onbewoond, onbewaakt en niet-beveiligd gebouw te worden geplaatst. Is het gebouw beveiligd en de brandkast voorzien van een tweede (cijfercombinatie)slot, dan kan aanzienlijk meer geld in de brandkast worden opgeborgen, of er kan voor een lichter type kast worden gekozen.

Wanneer de ontwerper weet om welk type brandkast het gaat, komen de bouwkundige zaken aan de orde waarop men attent moet zijn, zoals:

- de meest geschikte plaats, zowel uit het oogpunt van gebruik als beveiligingstechnisch;
- de vloerbelasting bij zwaardere typen;
- verankering in de vloer van lichtere typen;
- de bouwfase waarin de kast het best kan worden geplaatst enz.

De aanschaf van een brandkast

Een ieder die de zorg heeft voor waardevolle zaken wordt wel eens geconfronteerd met de vraag: hoe beveilig ik deze het best tegen brand en/of diefstal. Het antwoord is meestal simpel: berg ze op in een brandkast. Op dat moment beginnen meestal echter de problemen, omdat de brand- en/of inbraakwerende eigenschappen van de onderscheidene kasten zeer verschillend kunnen zijn. Bovendien is op dit gebied nogal wat spraakverwarring. Zo kennen wij naast de term 'brandkast' termen als 'brandwerende kast', 'in-

braakwerende kast' en 'kluis', terwijl deze begrippen elkaar toch niet dekken.

Het onderscheid tussen deze beveiligingsprodukten is in principe zo simpel als het klinkt, namelijk dat *brandwerende* kasten de inhoud ervan tot op zekere hoogte beschermen tegen brand, *inbraakwerende* kasten tegen inbraak en *brandkasten* tegen brand en inbraak, terwijl *kluizen* betonnen of gemetselde ruimten zijn, waarvan de wanddikte in overeenstemming is met het weerstandsniveau van de toe te passen deur. Verder wordt de term 'kluizen' ook wel gebezigd in het woord 'inbouwkluisen': als regel muurkluizen of vloerkluisen, waarbij de wijze van inbouw medebepalend is voor de weerstand. De benaming brandkast is eigenlijk wat ongelukkig; beter ware het te spreken van brand- en inbraakwerende kast, terwijl de aanduidingen *brandvrije* of *inbraakvrije* kast, waarvan sommige fabrikanten zich in hun folders bedienen, zelfs uit den boze zijn, omdat geen enkele kast deze beweerde eigenschap waarmaakt. Overigens is het onderscheid tussen brandwerende en inbraakwerende kasten, zeker voor de leek, veelal moeilijk te zien.

Waarvoor moet de kast dienen?

Bij een *brand* zal de kast de inhoud moeten beschermen tegen hoge temperaturen, eventueel een val (instorting van het gebouw of van een verdieping met kast en al) en bluswater. Bij een *inbraak* moet de kast weerstand bieden tegen inbraakwerktuigen. Bij de keuze van een kast dient men zich eerst goed te realiseren waarvoor de kast moet dienen. Wat moet beschermd worden en waartegen? In het hiernaast staande schema staat een overzicht van de diverse waardevolle zaken die bescherming behoeven, met de daarbij passende beveiligingsprodukten (middelen):

Fatale vergissing

Zoals al eerder aan de orde kwam, zien we dat normale brandwerende kasten, brandkasten of kluizen totaal ongeschikt

1 Beveiliging van conventionele administratie (beschreven of bedrukt papier)

Veilige temperatuurgrens:
165–175° C

Middelen:

- brandwerende kasten;
- brandwerende ladekasten;
- betonnen of gemetselde archiefkluizen met brandwerende archiefkluisdeuren.

2 Beveiliging van magnetische informatiedragers voor de computer (tapes, disk-packs en floppy-disks)

Veilige temperatuurgrens:

65–75° C,

bij floppy-disks zelfs 45–55° C

De relatieve vochtigheid dient onder de 85% te blijven.

Middelen:

- datasafes en diskettensafes;
- archiefkluizen van een speciale constructie, afgesloten door archiefkluisdeuren in combinatie met waterdichte deuren;
- archiefkluizen met brandwerende archiefkluisdeuren waarin voor additionele bescherming tegen verhitte en vocht speciale data-bewaarplaatsen worden geplaatst.

3 Beveiliging van geld en andere voor de inbreker interessante, waardevolle zaken

Het weerstandsniveau is afhankelijk van de waarde van de te beveiligen zaken.

Middelen:

- inbraakwerende kasten;
- brandkasten (brand- en inbraakwerende kasten);
- betonnen of gemetselde kluizen waarvan de wanddikte in overeenstemming is met het weerstandsniveau van de toe te passen kluisdeur;
- inbouwkluisen (muur- en vloerkluisen).

zijn voor het beveiligen van magnetische informatiedragers, zoals tapes en disks. Volkomen te goeder trouw worden deze vaak daarin opgeborgen, omdat men de waarde ervan meestal goed onderkent en men ze de 'veiligste' plaats op kantoor waard vindt. Maar de brandkast of brandwerende kast met zijn veilige temperatuurgrens van 165–175° C is dit zeker niet. Als er brand komt, zal blijken dat het een fatale vergissing is geweest.

Constructie van brandwerende kasten

In brandwerende kasten en deuren bevindt zich tussen de binnen- en buitenromp een materiaal dat meestal wordt aangeduid als brandwerende vulling. Dit materiaal moet ervoor zorgen dat de temperatuur in de kast, die bij brand buiten de kast kan oplopen tot $\pm 1.000^{\circ}\text{C}$, beneden de 165–175° C blijft. Bij deze temperatuur begint papier namelijk te verkleuren (oxideren). Het vocht dat zich in chemisch gebonden vorm in deze vulling bevindt, levert daar een belangrijke bijdrage aan. Wanneer de kast verhit wordt, betekent dit echter dat een gedeelte van dit vocht in dampvorm tot de inhoud van de kast kan doordringen. Dit zal voor papier in het algemeen geen bezwaar opleveren, maar het wordt duidelijk dat zaken die geen vocht kunnen verdragen (denk eens aan postzegels), niet zonder speciale voorzorgen in een normale brandwerende kast kunnen worden opgeborgen. Natuurlijk geldt het voorgaande ook voor de andere brandwerende middelen: laden-kasten en archiefkluizen.

Constructie van datasafes en diskettensafes

Het voorgaande verklaart reeds gedeeltelijk waarom een normale brandwerende kast niet geschikt is voor magnetische informatiedragers. De vochtigheidsgraad loopt te hoog op en we zagen al eerder dat de relatieve vochtigheid beneden de 85% moet blijven. Daar komt nog bij dat de temperatuur in de datasafe beneden de 65–75° C en in geval van berging van flop-

py-disks (diskettensafes) zelfs onder de 45–55° C moet blijven.

Aan deze eis kan voldaan worden door in de brandwerende kast een tweede kast in te bouwen die is opgebouwd uit droog isolerend materiaal. Deze kast dient zo hermetisch te sluiten dat ook geen vocht in dampvorm tot de inhoud kan doordringen.

Zekerheid door testen

Na een brand dient men de grootst mogelijke zekerheid te hebben dat alle beveiligde stukken en informatiedragers weer normaal te gebruiken zijn of vlot kunnen worden geproduceerd. Die zekerheid wordt alleen verkregen als men te doen heeft met brandwerende kasten die volgens strenge normen zijn getest. Bij de in het schema genoemde 'veilige temperatuurgrens' (165–175° C voor brandwerende kasten, 65–75° C voor datasafes en 45–55° C voor diskettensafes) is uitgegaan van de Duitse VDMA-norm naar RAL-RG 626/7. Dit houdt in dat de kast wordt getest bij een uitgangstemperatuur gelegen tussen minimaal 15° en maximaal 25° C en dat de binnentemperatuur van de kast gedurende de test niet meer mag stijgen dan de genoemde 'veilige temperatuurgrenzen'.

Een andere eis is dat de constructie solide genoeg is om bij instortende verdiepingen een flinke val te doorstaan, waarna de kast opnieuw aan het vuur kan worden blootgesteld. Neem nooit genoegen met de mededeling dat het produkt getest is. Er zitten grote verschillen in testduur en testmethoden. Het is zeker zinvol om altijd aan de fabrikant of leverancier het testrapport op te vragen.

Constructies van brandkasten, inbraakwerende kasten en (inbouw)kluizen

Bij de ontwikkeling van brandwerende kasten heeft de fabrikant te maken met duidelijk te definiëren risico's waartegen de constructie van de kast opgewassen moet zijn. Veel complexer ligt de zaak bij

kasten en (inbouw)kluizen die de inhoud (mede) tegen inbraak moeten beschermen. Deze moeten een veelheid aan inbraakwerktuigen en -methoden kunnen pareren. Het probleem dat zich daarbij voordoet, is dat een optimale beveiliging tegen het ene werktuig soms een minimale beveiliging tegen het andere werktuig betekent.

Op non-ferrometalen bijvoorbeeld, die zeer goede warmtegeleiders zijn en weinig affiniteit tot zuurstof hebben, kan men weinig uitrichten met een gewone oxy-acetylenebranders. Maar deze metalen zijn weer betrekkelijk zacht en dus niet zo moeilijk te boren. Ondanks zijn uitstekende eigenschappen is zo'n materiaal dus minder geschikt, tenzij het met hard materiaal wordt gepantserd. Een voorbeeld hiervan is aluminiumkorund, bestaande uit aluminium dat een zeer goede warmtegeleider is met daarin gegoten stukjes korund, een zeer hard, praktisch niet te boren materiaal.

Inbouwkluizen

Een aparte positie nemen de inbouwkluizen in. Inbouwkluizen zijn specifiek ontwikkeld voor de berging van goederen met een klein volume en een hoge waarde. Muurkluizen zijn algemeen bekend vanuit literatuur en filmwereld; de huidige bouwmethoden en gebruikte materialen bieden echter nauwelijks mogelijkheden om een muurkluis effectief in te bouwen. Vloerkluizen zijn 'herontdekt', dat wil zeggen dat de mensheid de grond altijd al heeft gebruikt als veilige bergplaats voor uiteenlopende zaken zoals voedsel, bezittingen, geheimen enz. De duidelijke voordelen van een vloerkluis zijn de 'verborgen veiligheid' onder vloerbedekking. De vloer is doorgaans het laagste punt in een pand en geeft derhalve ook een goede bescherming tegen brand. De vloerkluis wordt rondom in beton gegoten, waardoor de deur verzonken in de vloer is gesitueerd. Dit is een uitermate goede beveiliging omdat de aan te vallen deur een klein oppervlak heeft én omdat men moet werken met inbrekerswerktuigen op een

in de vloer verzonken kluisdeur. Aangezien een inbouwkluis massief met de woning of het pand is verbonden zal deze niet snel meegenomen kunnen worden, daar de inbreker gebruik zal moeten maken van hak- en sloopwerktuigen om de kluis uit zijn betonnen ommanteling te krijgen. Afgezien van de permanente waardeberging die een vloerkluis biedt, wordt de vloerkluis de laatste jaren meer en meer toegepast als tijdelijke bergplaats ter bescherming tegen overval en kaslichting. Daarom zijn veel vloerkluizen uitgerust met een inwerpmechanisme of deposit-systeem (waarover direct meer).

In de laatste jaren zijn er tevens vloerkluizen ontworpen met een rechthoekige deur voor de berging van volumineuze artikelen zoals ordners, juwelenkisten, zilveren serviezen en dergelijke. De rechthoekige deur heeft echter het nadeel dat deze makkelijker is aan te vallen vanwege zijn grotere oppervlak in vergelijking met de ronde-deurtypes.

Van groot belang is natuurlijk de kwaliteit van de inbouw van de kluis. Het dient benadrukt, dat slechts gesproken kan worden van een goede beveiliging indien de inbouwkluis ook goed is geïnstalleerd. Slechts enkele leveranciers verstrekken een 'Certificaat van installatie' bij inbouw van een muur- of vloerkluis. Het is dus van belang hiernaar vooraf te informeren.

Resumerend kan gesteld worden dat een inbouwkluis of een vloerkluis een goede en afdoende beveiliging tegen brand en inbraak kan zijn als het gaat om middelmatige hoeveelheden geld en andere waardestukken die, hetzij permanent, hetzij als daggeldberging veilig opgeborgen dienen te worden.

Ten slotte nog een vergelijking met de gebruikelijke brandkasten: een vloerkluis is verborgen veiligheid, neemt geen ruimte op de vloer in en kost de helft tot een derde van de prijs van een gelijkwaardige brandkast. Hier staat echter tegenover dat een vloerkluis ingebouwd dient te worden, een beperkte ruimte biedt en een relatief kleine opening heeft.

Inwerpmechanisme

Brandkasten zijn in principe ontworpen om de inhoud ervan tegen brand, diefstal en inbraak te beschermen. Op het diefstal- en overvalrisico gedurende werkdagen (kasuren) zijn zij normaal niet berekend. Immers, de brandkast zal dan veelal niet afgesloten zijn, althans de sleutel zal ter plaatse aanwezig zijn. Een snelle greep in de kas(t) door een overvaller of een onbetrouwbaar personeelslid of het dwingen de kast te openen, behoren dan tot de mogelijkheden. Soms kan men dit onderwerpen met een tijdslot. Maar wanneer men regelmatig in de brandkast gelden moet afstorten, schiet dit middel aan zijn doel voorbij.

Brandkastenfabrikanten losten dit probleem op met de ontwikkeling van een cassetteinwerpmechanisme, ook wel de posit-systeem geheten. Dit is een voorziening bestaande uit een inwerpopening in de kast, waarin cassettes, eventueel enveloppes en dergelijke, via een 'kanaal' in de kast kunnen worden gedeponeerd. Bij een goede constructie wordt het beveiligd vermogen van de kast niet aangetast: dit houdt onder meer in dat het kanaal in de kast voorzien is van een sluisstelsel, waardoor 'hengelen' via de inwerpopening, ook als de kast bijvoorbeeld vol water wordt gepompt, onmogelijk is. De inwerpopening zelf is doorgaans afgesloten met een deur of een klep. Ook de cassettes zijn afsluitbaar.

Dit maakt het mogelijk om ook als de deur gesloten is geld in de brandkast kwijt te kunnen. Het systeem is er uiteraard op gebaseerd dat de sleutel- en/of de cijfercombinatiecode niet in de omgeving van de brandkast voorhanden zijn. Hiermee wordt een doeltreffende beveiliging tegen diefstal en overval gerealiseerd als verlengstuk van de beveiliging die de brandkast normaliter al biedt.

Brandkasten met inwerpmechanisme bieden nog een extra gebruiksmogelijkheid. Vertegenwoordigers of chauffeurs die na normale kasuren geld moeten afdragen, kunnen dit doen via de brandkast met inwerpmechanisme. Er behoeft dan ge-

durende de avonden geen menskracht beschikbaar te zijn als 'oppas' bij de brandkast om de deur te openen en te sluiten.

Dit bespaart niet alleen extra tijd en kosten, maar er wordt ook mee voorkomen dat een situatie ontstaat die bijzonder gunstig is voor een overval. (Bij bankinstellingen is dit systeem al jaren ingeburgerd: nachtkluizen.)

Een bijkomend voordeel is dat men door het kunnen deponeren van geld in de brandkast de hoeveelheid geld in de kassa-lade (denk aan onder meer winkelbedrijven, bezinestations en dergelijke) beperkt kan houden tot uitsluitend het wisselgeld; wederom een situatie die weinig attractief is voor een overvaller.

Sleutelstot

"De brandkast werd geopend met de sleutel die men in een bureaulade vond" kan men regelmatig in de pers lezen. Het is volkomen terecht dat verzekeraars normaliter de eis stellen dat de sleutel niet mag worden opgeborgen in het gebouw waar de brandkast staat. Maar ook al springt men uiterst zorgvuldig met de sleutel om, het blijft toch altijd een veel eenvoudiger zaak een brandkast sleutel te veroveren dan een brandkast te kraken. Als men de sleutel heeft, staat de brandkast bij wijze van spreken open. Maar er is meer. Alle sleutelstoten zijn in principe kwetsbaar, omdat het zwakke punt het sleutelgat is. Dit maakt het mogelijk om bijvoorbeeld met explosieven, chemicaliën of gereedschappen in het slot te komen. Hiermee zij niet beweerd dat fabrikanten hiertegen geen maatregelen hebben getroffen. Een goed geconstrueerde kast kent voorzieningen, waaronder een zogenaamde actieve noodshoot, die de deur in gesloten toestand houden bij een aanval op het slot.

Cijfercombinatieslot

Het 'sleutelrisico' brengt met zich mee dat het belangrijk is dat een brandkast is uitgerust met een cijfercombinatieslot als

tweede slot. Door het zeer grote aantal combinatiemogelijkheden (veelal een miljoen of meer) is het praktisch uitgesloten om de combinatie te vinden. Films, waarin de inbreker soms met gebruikmaking van een stethoscoop het aantal hoorbare klikken aftelt en op deze wijze binnen een korte spanne tijds de combinatie vindt, geven een vals beeld van het moderne cijferslot. Verder is het mogelijk om een zogenaamde spy-proofring rond het slot aan te brengen die het onmogelijk maakt om over iemands schouder de combinatie mee te lezen wanneer deze gedraaid wordt. Mocht er nochtans een vermoeden bestaan dat onbevoegden de juiste combinatie kennen, dan hoeft men slechts een nieuwe combinatie in te stellen. Dit laatste verdient ook aanbeveling bij personeelwisselingen. Een bijkomend voordeel van een cijfercombinatieslot boven een sleutelslot is dat er zich geen kwetsbare opening (sleutelgat) in de deur bevindt.

Tijdvertragingsslot

Een specifieke vorm van beveiliging tegen overval gedurende de openingstijd van het pand waar een inbraakwerende kast in gebruik is, is het tijdvertragingsslot. Gekoppeld aan het sleutelslot of cijfercombinatieslot berust de werking op het principe van vertraging; op het moment dat het slot wordt opengedraaid, stelt men een tijdmechanisme in werking (zelf instelbaar van 1 minuut tot 1 uur). De kast zal pas te openen zijn ná afloop van de ingestelde vertragingstijd.

Tijdslot

Het tijdslot is enorm in opmars. De oorzaak is te vinden in de harder wordende criminaliteit, waarbij veel vaker dan vroeger sprake is van bedreiging met vuurwapens. Een methode om de inhoud van een brandkast te bereiken, is de eigenaar of beheerder te dwingen de brandkast open te maken. Dit risico is vooral groot in situaties waarin de beheerder boven of naast het pand, waarin de brandkast staat

opgesteld, woont. Met het tijdslot kan men de deur van de brandkast gedurende een vooraf in te stellen tijdsduur voor iedereen gesloten houden, ook al zouden cijferslot en sleutelslot in geopende stand zijn. De beheerder van de brandkast kan dus ook niet onder bedreiging gedwongen worden de deur te openen zolang de ingestelde tijdsduur niet verstreken is. Een tijdslot heeft als regel twee of drie chronometers die kunnen worden ingesteld op maximaal 144 uur of wel zes etmalen. Een bijkomend voordeel van een of meer extra sloten is dat verzekeraars dit als regel honoreren met een hogere dekking of een lagere premie.

Sluitmechanisme

Zonder hier al te diep op in te gaan is het wel nuttig te memoreren welke eisen men aan het sluitmechanisme moet stellen. Hoe zwaar en solide een brandkast immers ook is geconstrueerd, als de deur op enigerlei wijze open te krijgen is, helpen de pantsermaterialen in de romp en de deur geen zier. Het sluitmechanisme dient zodanig te zijn geconstrueerd dat, wanneer men er al in zou slagen de sloten te verwijderen of te vernielen door middel van explosieven of andere werktuigen, de gesloten stand van de 'schoten' onverminderd gehandhaafd blijft. Bovendien dient een goed sluitmechanisme te zijn voorzien van een actieve noodshoot, die bij aanvallen met explosieven, thermische lansen of andere warmsnijdende werktuigen de uitschuivende schoten van het sluitwerk extra blokkeert.

Kluisdeuren

Hetgeen is gezegd over brandwerende kasten en inbraakwerende kasten geldt in principe ook voor brandwerende archiefkluisdeuren en inbraakwerende kluisdeuren. Een wezenlijk verschil is dat een kluisdeur voorbestemd is een stuk onroerend goed te worden dat in de bouwfase wordt verwerkt. Een brandkast moet een door deuren of ramen te transporteren produkt blijven en om in zo'n kast ook nog

opbergruimte over te houden, blijft de dikte van deur en romp — en daarmee ook het weerstandsvermogen — aan beperkingen gebonden. Bij kluisdeuren is het mogelijk materiaaldikten veel verder op te voeren. Daarom is voor zeer hoge risico's de betonnen kluis met zware kluisdeur de aangewezen beveiliging.

Eisen te stellen aan brandkasten en inbraakwerende kasten

Niet alle kasten bezitten de gehele scala van pantsermaterialen en anti-inbraakvoorzieningen die hier zijn op te sommen, dus niet alle kasten zijn even inbraakwerend. En het is goed dat er verschil is — ook prijsverschil — want het is logisch dat men anders aankijkt tegen een beveiliging van f 100.000,- in contant geld dan tegen een kas van vijf- of tienduizend gulden. Bovendien is de *lokatie* van belang. Een brandkast in het hoofdbureau van politie levert een ander risico op dan een kast in een 's nachts verlaten kantoor. Verder is de *leeftijd* van de kast van belang. De brandkastfabrikant dient namelijk adequaat in te spelen op de ontwikkeling in de technologie en de veranderende inbraaktechnieken. Voorbeelden van dit laatste zijn onder andere de diamantboor,

waarmee kaarsrechte gaten met een grote diameter in beton geboord kunnen worden, en de thermische lans die vooral de laatste tien jaar ruime bekendheid hebben verkregen als inbraakwerktuig. Het is hierdoor duidelijk dat een brandkast die vervaardigd is aan het begin van deze eeuw, of zelfs in de jaren vijftig, niet die mate van bescherming kan bieden als de brandkasten die in de jaren tachtig worden gemaakt. Dit betekent allerm minst dat alle brandkasten met een leeftijd van circa 25 jaar of ouder hierdoor waardeloos zijn geworden; een en ander houdt echter wel in dat dit soort brandkasten beter niet kan worden gebruikt voor de beveiliging van zeer waardevolle zaken of veel contant geld. Vaak voldoen deze kasten echter nog goed als brandwerende beveiliging, zolang het maar niet om de bescherming van magnetische informatiedragers gaat.

RUIMTEN VOOR GELDZAKEN

Zodra er veel contant geld in een kantoor omgaat, ontstaat al gauw de behoefte aan een ruimte waar men veilig en in alle rust geld kan tellen en eventueel aan een kas-sier kan afdragen. Hier ontbreekt het nogal eens aan, met alle gevolgen van dien.

links:

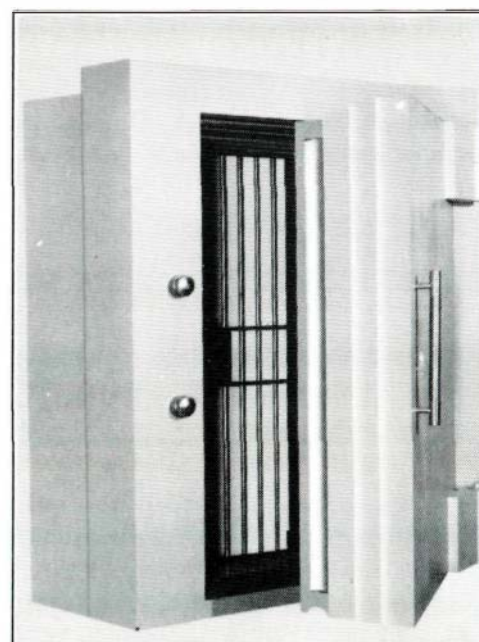
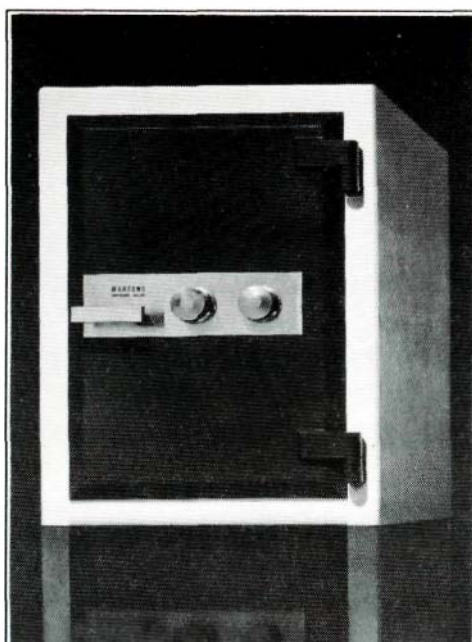
Brandkast in traditionele uitvoering; brand- en inbraakwerend

midden:

Kluisdeur

rechts:

Inbouw (vloer)kluis



Een dergelijke ruimte moet goed afsluitbaar zijn, en van buiten en binnenuit het kantoorgebouw moeten buitenstaanders niet in deze ruimte kunnen kijken. Anderszins moet er toch de mogelijkheid zijn dat bevoegden (bijvoorbeeld de kassier)

desgewenst op de situatie in deze ruimte kunnen toezien. Dat wordt bijvoorbeeld gerealiseerd door de deur in het door een toegangscontrolesysteem beveiligde gebied te projecteren en te voorzien van een kleine ruit van slagwerend glas. Deze deur



zou bijvoorbeeld in de nabijheid van de toegangsdeur van de kassiersruimte kunnen worden gesitueerd.

Intern en extern geldtransport

Op een gegeven moment zal het teveel aan geld uit het kantoorgebouw moeten worden afgevoerd naar een bank, waarvoor in toenemende mate gespecialiseerde geldtransportbedrijven worden gebruikt. De route tussen de plaats in het kantoorgebouw waar het geld is opgeborgen en de geldtransportauto is soms te lang. Bij nieuw- of verbouw is het dus wenselijk erop attent te zijn het interne geldtransport in het kantoorgebouw, en daarna buiten tot aan de geldtransportauto, zo kort mogelijk te houden.

Ideaal is een eigen parkeerplaats voor deze auto, waarbij deze zo dicht mogelijk tegen de gevel geparkeerd kan worden. Direct achter dit (blinde) geveldeel bevindt zich de ruimte die naar de geldberging, en de eventueel aanwezige kassieren geldtelruimte leidt. Via een voor dit doel geschikt stalen luik in het betreffende geveldeel waar de auto staat geparkeerd kan het geld worden afgevoerd.

Wanneer het minder eenvoudig blijkt plaatsen met geldhandelingen, geldtelruimte, kassiersruimte, geldberging enz. op relatief korte afstand van elkaar te projecteren, kan het risico van het interne geldtransport worden beperkt door toepassing van een voor dit doel geschikt buizenpoststelsel. Mits in voldoende mate beveiligd zou een dergelijk stelsel ook voor collectief gebruik in een kantoorcentrum met een bankfiliaal toegepast kunnen worden.

BEWAKINGSRUIMTEN

Onder bewakingsruimten wordt hier verstaan de groep van ruimten die een specifieke functie in de beveiliging van een kantoorgebouw hebben. Dat kunnen zijn een meldkamer, portiersloge, ruimte voor personeel van een eigen of ingehuurd bewakingsdienst enz.

Meldkamer

De hier bedoelde meldkamer is een soort alarmcentrale voor eigen gebruik en heeft niets van doen met de eerder genoemde particuliere alarmcentrale (PAC).

Een PAC exploiteert zijn meldkamer voor derden. Men kan er via het telefoonnet bijvoorbeeld het inbraaksignaleringssysteem op aansluiten, en bij alarm brengt de PAC de vantevoren afgesproken communicatie en hulpverlening op gang.

De eigen alarmcentrale of meldkamer zal afhankelijk van de omvang van de beveiligingsactiviteiten in het kantoorgebouw (of het complex van kantoorgebouwen) sterk in omvang en inrichting uiteenlopen. Op het moment dat er meerdere systemen in het kantoorgebouw zijn die direct met beveiliging te maken hebben, zoals een gesloten televisiecircuit, inbraaksignalering, een controlesysteem op bewakingsronden, een toegangscontrolesysteem, draadloze communicatiesystemen enz., zal al gauw een eigen centrale ruimte voor deze systemen gewenst zijn. Veelal monden voornoemde systemen uit in kleine computerachtige eenheden met monitoren, printers, ontvangers en (video)recorders. In de meldkamer kan de apparatuur centraal worden ondergebracht en beheerd. Bij een wat grotere omvang van het beveiligingsgeheel zal de ruimte permanent zijn bemand. Deze ruimte is ook bij uitstek geschikt om speciale hulpmiddelen voor de beveiliging op voorraad te houden.

De meldkamer moet binnen het kantoorgebouw op een rustig punt worden gesitueerd, en bij voorkeur zo ver mogelijk verwijderd liggen van de hoofdingang of mogelijke andere in- of uitgangen. De meldkamer moet zo gesitueerd zijn dat men niet vanuit belendende gebouwen naar binnen kan kijken. Eventueel zijn hiervoor niet-bouwkundige voorzieningen toepasbaar. Ten aanzien van de benodigde ruimte voor een meldkamer wordt gedacht aan minimaal 20 m² plus 6 m² voor het opstellen van apparatuur.

Meldkamers dienen, afhankelijk van de bezettingsgraad, bij voorkeur te worden

uitgerust met een eigen toilet en een kleine pantry. De omsluitende wanden en vloeren van de meldkamer dienen bij voorkeur 'hard' en blind te zijn, terwijl de toegang tot deze ruimte moet geschieden door middel van een toegangssluis (zie ook hoofdstuk 10). Toegepast glas moet in voldoende mate slagwerend zijn. De aan- en afvoergoten van kabels en dergelijke dienen te worden afgeschermd tegen sabotage, of in de muren te zijn weggewerkt. Het spreekt voor zich dat de meldkamer en de directe omgeving een belangrijk onderdeel vormen van het (toegangs)beveiligingsplan.

Portiersloge

De portiersloge vormt een onderdeel van de entree. Deze uit veel glas opgetrokken ruimte zal zoveel mogelijk inbraak- en slagwerend moeten worden uitgevoerd. In grote lijnen gelden voor het ontwerp dezelfde uitgangspunten als bij de hiervoor besproken meldkamer, zij het dan dat hier met veel glas zal worden gewerkt. In deze ruimte staat vaak ook apparatuur opgesteld die direct aan de hiervoor genoemde meldkamer is gekoppeld, danwel dat bepaalde gegevens uit de meldkamer of elders automatisch aan de portiersloge worden doorgegeven. Hier bevindt zich ook altijd een paneel van het branddetectiesysteem.

De beveiligingstechnische detailuitvoering van de portiersloge zal geheel afhankelijk zijn van het beveiligingsniveau in het betreffende kantoorgebouw. Is dit hoog dan zal de constructie rondom als 'schil' geheel gesloten moeten zijn, met een daarop afgestemde klimaatregeling. Is het niveau zeer laag, dan kan de constructie gedeeltelijk open zijn.

Ruimten voor bewakingspersoneel

Geheel afhankelijk van de beveiligingsorganisatie rond een kantoor (gebouwen-complex) zal er meer of minder behoefte zijn aan een eigen ruimte voor bewakingspersoneel. Hier ligt de nadruk niet op beveiliging van de ruimte zelf, maar meer

in het beheer van het eigen of ingehuurde bewakingspersoneel.

Een dergelijke ruimte vraagt bijvoorbeeld ook om een eigen toilet en een kleine pantry. In situaties waarbij ingehuurd bewakingspersoneel na sluitingstijd niet het kantoorgebouw in hoeft, gaat de voorkeur uit naar een niet in verbinding met het kantoorgebouw staande aanbouw, of een voor dit doel geschikte 'portacabin' op het terrein.



Bezit dient men meestal achter goed gesloten deuren te beschermen. Alhoewel een oud Chinees spreekwoord zegt: “De best gesloten deur is die welke men open kan laten staan”, is die filosofie voor de beveiliging van gebouwen in de westerse samenleving nooit bruikbaar geweest, evenmin trouwens als het bekende blauwe bord met “Verboden Toegang”. Ter bescherming van bezit moeten we toezicht houden op die deur of hem gewoon goed afsluiten. Eeuwen achtereen is dit met zeer uiteenlopende constructies gedaan die we sloten noemen: mechanismen die ervoor dienen om snel en gemakkelijk een verbinding tot stand te brengen tussen een beweegbaar en een vast gedeelte, ofwel tussen een deur en een kozijn. Uitgangspunt daarbij is steeds weer dat de verbinding door onbevoegden niet of zeer moeilijk te verbreken mag zijn. Is iedereen die een passende sleutel heeft nu bevoegd?

Een na werktijd verlaten kantoorgebouw vormt een inbraakrisico.

Inbraakbeveiliging moet dit risico afdekken. Gedurende werktijd is het gebouw evenwel vol mensen en de beveiliging zal zich dan moeten toespitsen op de kwetsbare ruimten, vooral op die waar het een continu komen en gaan van mensen betreft.

Niemand zal er overdag over denken een deur of een slot te forceren of een ruit stuk te slaan; immers de kans om op heterdaad betrapt te worden is veel te groot. Onbevoegden zullen hun kans dan ook afwachten. Het risico wordt hier dus gevormd door mensen die op geen enkele manier de aandacht willen trekken.

Dit risico moet worden afgedekt met *toegangscontrole*.

Op de meest belangrijke aspecten van deze beveiligingsvorm wordt in de volgende hoofdstukken ingegaan.

TOEGANGSCONTROLE

In de praktijk komen we de toegangscontrole in en rond gebouwen vaak tegen in de vorm van een planmatige aanpak van de controle op alle toe- en uitgangen. Men spreekt dan van een *toegangscontrolesysteem*. Hart van het systeem is dan doorgaans een microcomputer. Maar we kunnen toegangscontrole ook aantreffen in de

vorm van één of meerdere deuren die zijn voorzien van bijvoorbeeld een codeslot.

Wat we als toegangscontrole steeds minder zien is de ‘portier’ per belangrijke toe- of uitgang. Daarvoor in de plaats komt steeds meer de professionele bewaker die met technische hulpmiddelen zoals portofoon, gesloten televisiecircuit, toegangscontrolesysteem enz. heel wat meer aan kan dan zijn voorganger de ‘portier’.

Een toegangscontrolesysteem biedt in dit verband dan ook nog het voordeel dat het zuiver ‘logisch’ werkt, en (doorgaans) nooit zo faalt als een menselijk (emotioneel) systeem.

Een portier kent vaak niet iedereen even goed die door de toegang gaat die hij bewaakt en misschien kent hij enkele mensen juist te goed. Het is een voordeel dat het toegangscontrolesysteem iedereen gelijk behandelt en de bewaker de gelegenheid krijgt taken op zich te nemen waarvoor hij uit hoofde van zijn functie beter geschikt is.

Alvorens in te gaan op de meer uitgebreide toegangscontrolesystemen staan we stil bij enkele vormen van toegangscontrole die in principe ook in vele wat meer kleinschaliger situaties goed toepasbaar zijn. Hierbij wordt gedacht aan sloten met cilinders, in een systeem waarbij het ‘bevoegd zijn’ in de sleutel ligt opgesloten.

SLOTEN EN SLEUTELDISCIPLINE

Elke beveiliging met sloten faalt als sleutels zoekraken of onbeheerd blijven liggen. In korte tijd kan iemand een afdruk van een sleutel maken of hem laten kopiëren in één van de vele 'sleutelbars'. Sleutels met een beschermd profiel zijn in dit opzicht wel iets veiliger, maar veelal is de bescherming in de praktijk slechts van tijdelijke aard.

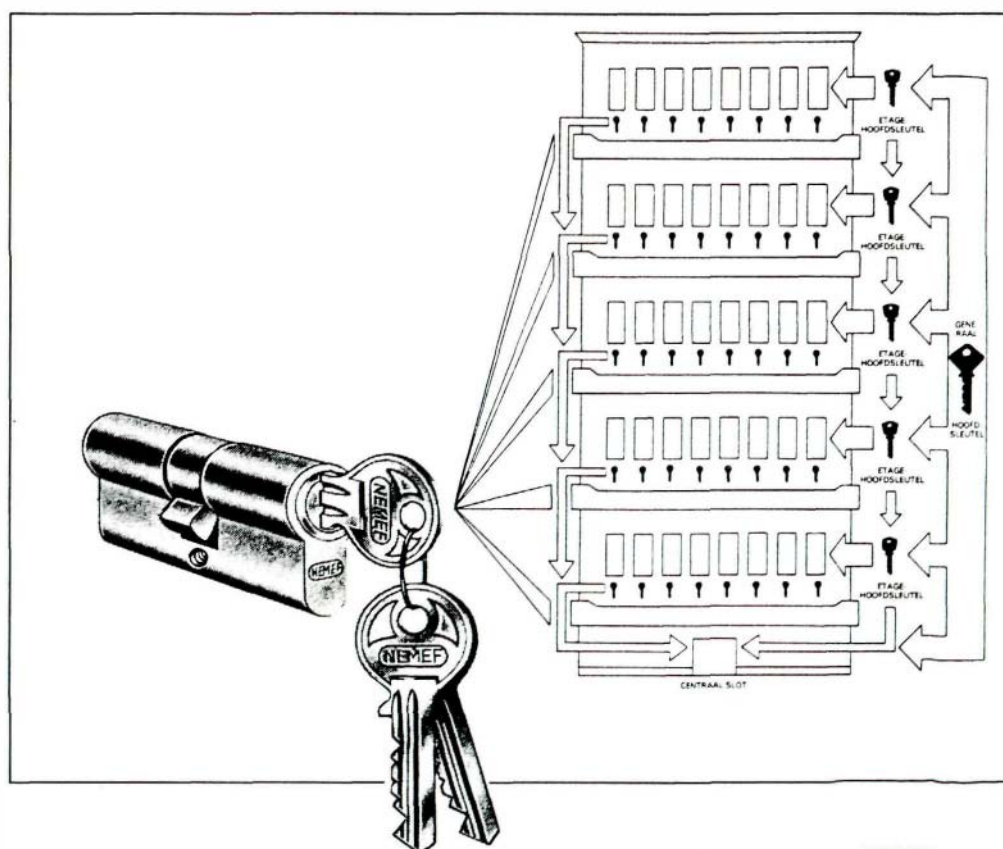
Alle bestaande sleutels van belangrijke sloten in een kantoor moeten zijn geregistreerd en van uitlenen en terugbezorgen moet aantekening worden gehouden. De gebruiker moet de sleutels steeds bij zich dragen of opbergen in een kast met op z'n minst dezelfde graad van beveiliging als het slot waar de sleutel op past. De sleutel van die kast moet hij dan steeds bij zich dragen, bij voorkeur aan een sleutelketting. Bij vermissing van sleutels of bij verdenking van het maken van ongeregistreerde kopieën is het nodig de betreffende cilinder van het slot door een ander in het systeem passend exemplaar te vervangen.

SLOTEN ZONDER SLEUTEL

Er zijn ook sloten zonder sleutels. Bekend is het cijfercombinatieslot op brandkasten en kluisdeuren, maar er zijn ook normale bouwsloten die een ingebouwd druktoetsenpaneel hebben. In beide gevallen dient een bepaalde cijfercombinatie met behulp van de druktoetsen (soms met een draaischijf zoals van een telefoontoestel) te worden ingevoerd. Dit soort sloten is bijzonder geschikt voor de situatie waarin slechts één of een klein aantal deuren qua toegang moeten worden beveiligd, zoals bijvoorbeeld een klein magazijn, een ruimte met gevaarlijke stoffen, een kast voor de technische dienst of de schoonmaakdienst, een archief enz.

Al speelt sleuteldiscipline hier geen rol, men zal de cijfercombinatie natuurlijk goed moeten beschermen. Dat laat in de praktijk nog wel eens wat te wensen over. In vele gevallen treft men in kantoren de cijfercombinaties van brandkasten in agenda's of onder de bureau-onderleggers aan!

*Schema voor
sluitsystemen*



Sloten zonder sleutel



In het geval van de druktoetssloten is het niet altijd te voorkomen dat iemand over de schouders van de gebruiker meekijkt, zodat de cijfercombinatie meestal snel bekend is. Bij dergelijke sloten kan de combinatie overigens meestal vrij gemakkelijk worden veranderd. Een aantal sloten heeft een zodanige uitvoering van het toetsenpaneel dat 'meelezen' zeer moeilijk of onmogelijk is.

SLOTEN MET KAARTEN

Een toegangsbeveiligingsvorm die we steeds meer toegepast zien, is het slot dat met een kaart wordt bediend. Wat is het verschil tussen een kaart en een sleutel? De kaart wordt in een gleuf op het slot of van een 'kaartlezer' nabij de deur gestoken, ofwel in de nabijheid van een al of niet zichtbare kaartlezer gehouden. In de kaart is een aantal gegevens in code opgeslagen. Zodra deze gegevens overeenstemmen met die van de kaartlezer c.q. die van de computer waaraan de kaartlezer is gekoppeld, wordt de toegang vrijgegeven doordat:

- de knop of krakblokkering wordt opgeheven zodat men de dagschoot kan bedienen;
- de schoot door een spoel wordt ingetrokken;
- de sluitplaat wordt vrijgegeven door een elektromagneet
- de schoot door een elektromotor wordt teruggetrokken.

Afhankelijk van de inbraakwerende eisen wordt dit 'vrijgeven' van de schoot toegepast op dagschoot, nachtschoot of een gecombineerde dag- en nachtschoot.

De gecodeerde kaartgegevens kunnen op velerlei manieren in de kaart zijn opgeslagen. Dit kan bijvoorbeeld in de vorm van geponste gaatjes, zoals bij een Hollerith-kaart waarbij het systeem mechanisch kan werken (bijvoorbeeld de mechanische kaartlezer), maar ook op elektronische wijze kan de gaatjescodering worden gelezen. Voor het merendeel zijn de gegevens evenwel op niet-zichtbare wijze aangebracht en hebben we te maken met een

hardplastic kaart in de creditcard-afmetingen van (85,5 x 54 mm) en soms in het badgecardformaat van (59 x 82 mm, dat is 1/3 ponskaart).

Deze kaarten zijn uit een aantal lagen opgebouwd. De laag met gegevens in het hart van de kaart is doorgaans niet anders te bereiken dan door de kaart te vernielen. De min of meer beruchte fraudebestendigheid speelt ook hier — net als bij de paspoorten — een rol. Deze rol is natuurlijk sterk afhankelijk van het totale beveiligingsniveau van het toegangsbeveiligingsplan. Zaak is natuurlijk dat de kaart niet op eenvoudige wijze kan worden nagemaakt.

De gegevens 'in de kaart' kunnen daar op zeer uiteenlopende wijze zijn ondergebracht met toepassing van soms zeer verregaande lees- of herkenningstechnieken zoals bijvoorbeeld:

- ponsgaatjes (Hollerith);
- zichtbare opdruk zoals barcode;
- magneetstrip;
- magneetpunten;
- resonantiekringen;
- lichtdoorlaatbaarheid;
- draadjes in bit-patroon (Wiegand-effect);
- infrarood;
- inductie (statisch of dynamisch);
- micro-reliëf (hologram);
- magnetisch 'watermerk';
- laser;
- geïntegreerde schakeling (chip- of 'smart'-kaart);
- combinaties van twee of meer hiervoor genoemde leestechieken.

Bij enkele technieken hoeft de kaart slechts in de buurt van de kaartlezer te komen, de zogenaamde 'hands-free'-systemen. De meest voorkomende varianten hiervan zijn de kaart met een statisch resonantiecircuit, de kaart met een actieve schakeling, die een code uitzendt zodra deze in de buurt van de kaartlezer (zender/ontvanger) komt en de wat dikkere 'kaart' die in feite als normale zender werkt.

De gebruikelijke kaart (credit- of badgeformaat) is aan de buitenzijde veelal uit-

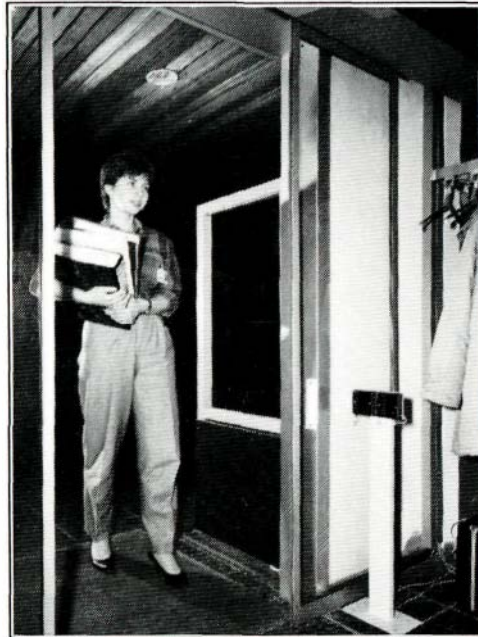
gevoerd als legitimatiebewijs met een foto van de houder. Net als bij de sleutel moet de kaart niet zoekraken of onbeheerd blijven liggen.

PERSOONSGEBONDEN TOEGANGSCONTROLE

Om te voorkomen dat anderen de kaart misbruiken, bijvoorbeeld na diefstal of verlies, wordt vaak nog een persoonlijke code vereist die men ter plaatse van de kaartlezer op een druktoetsenpaneeltje moet invoeren.

Maar ook deze extra veiligheid heeft haar beperkingen. Een zeer veilig systeem is dat van de persoonsgebonden toegangscontrole. Hierbij wordt ook een kaart gebruikt maar wordt tevens gecontroleerd of het wel de echte kaarthouder is die hem gebruikt. Dit kan men doen door middel van toetsing van typische lichaamskenmerken van de kaarthouder, zoals gewicht, lengte, handpalm, vingerafdruk, stem, gezichtsvorm enz.

Aangezien deze vorm van persoonlijke codering moeilijk valt te saboteren, kan met dit soort systemen een zeer hoge graad van beveiliging worden bereikt. Men past deze systemen natuurlijk alleen



*'Hands-free'-systeem
(kaart op blouse gespeld)*

toe waar dit qua beveiligingsniveau noodzakelijk is.

COMPLETE TOEGANGSCONTROLE

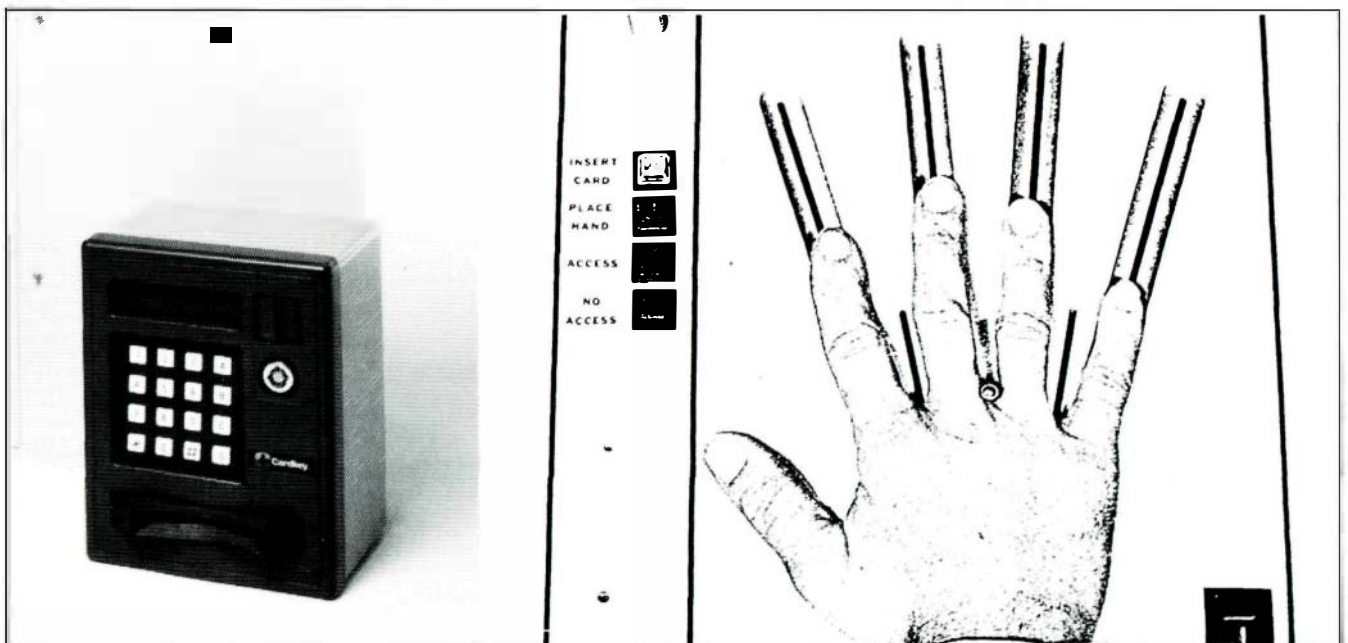
Bij de enkelvoudige toegangsbeveiliging waarin alle technieken ten behoeve van één toe- of uitgang in één unit zijn ondergebracht, waaronder bijvoorbeeld een

links:

*Kaartlezer met
persoonlijke code*

rechts:

*Persoonsgebonden
toegangscontrole*



kleine microcomputer, spreekt men van een 'off-line'-systeem ofwel een 'stand-alone'-eenheid. Of het systeem nu in meer of mindere mate mechanisch en/of elektronisch is uitgevoerd, het behoort vrijwel altijd tot de categorie 'slot met kaart'. Met een dergelijk systeem kan men bijvoorbeeld één deur of de slagboom van een parkeerterrein beheren. Vaak gaat de wens naar de gecontroleerde toe- en uitgang verder dan alleen het signaleren of er iemand binnenkomt of uitgaat. Eigenlijk wil men steeds wel weten wie binnen waarheen gaat en het liefst ook nog via welke route, wanneer en waarom. Dit kan voor het merendeel worden bereikt met behulp van de meer uitgebreide toegangscontrolesystemen. Men gaat dan uit van een grotere computereenheid die als het 'intelligente hart' van het systeem dient en waarop alle kaartlezers worden aangeslo-

ten. Niet alleen de buitendeuren, maar alle deuren in het kantoorgebouw die bij belangrijke ruimten horen (als computer-ruimte, kluisruimte, research-afdeling, magazijn) of anderszins van strategisch belang zijn worden dan bewaakt. Bij een dergelijk systeem (men spreekt dan van 'on-line') is het bijvoorbeeld mogelijk:

- een presentlijst af te drukken van alle binnenkomende personen, met de exacte tijd van binnenkomst, c.q. de tijd van vertrek;
- een absentielijst te produceren;
- automatisch bepaalde personen bij binnenkomst te laten oproepen wanneer dit gewenst is;
- de toegang met variabele parameters te laten functioneren: bijvoorbeeld door de toegang tijdens bepaalde dagen of uren automatisch te blokkeren;
- meldingen op lijsten af te drukken met



tijdstip (sabotagemelding, technische melding enz.);

- speciale toegang te verlenen met behulp van de kaart én een op de kaart-lezer in te toetsen (variabele) code.

Andere zaken dan de beveiliging kunnen ook worden 'meegenomen' zoals:

- kantinegebruik en afrekening;
- gebruik van een eigen bedrijfsbenzinepomp, al dan niet met afrekening;
- gebruik kopieerapparatuur, koffieautomaten enz.

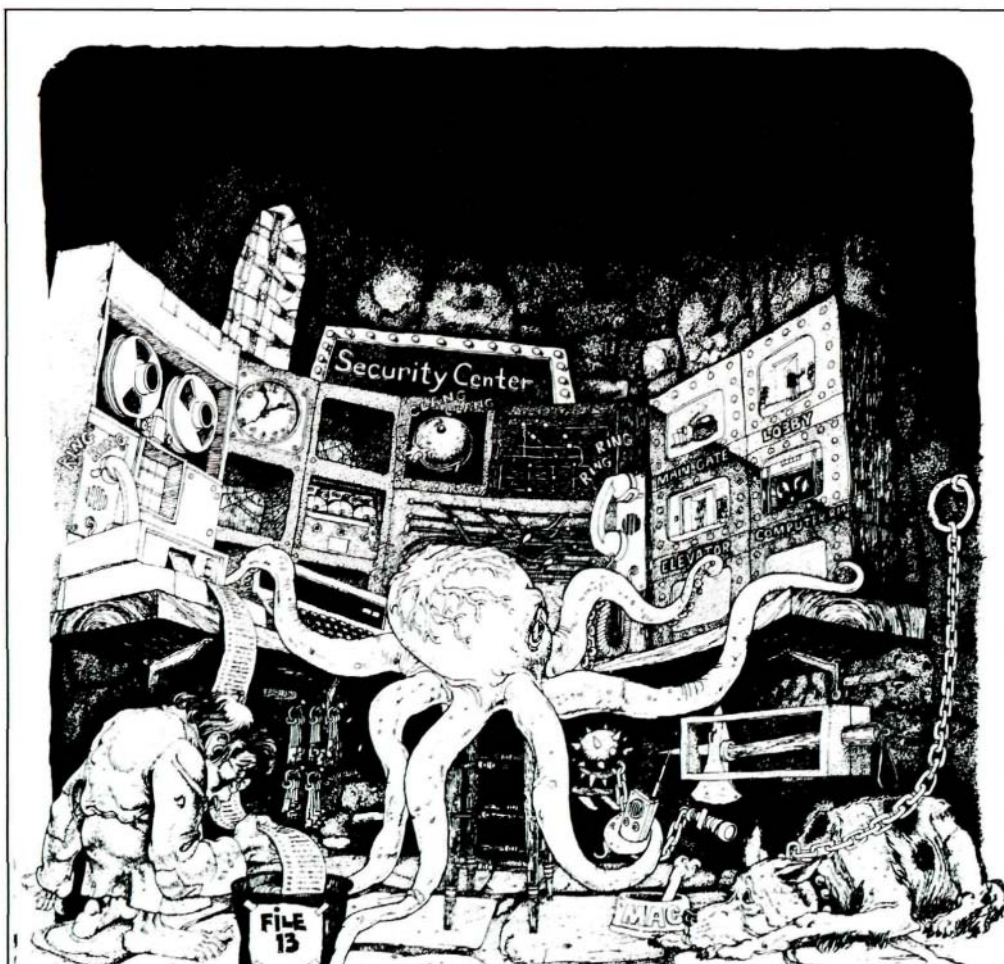
DE TOEKOMST

Het wordt langzamerhand duidelijk dat beveiligingsinstallaties in de toekomst meer en meer geïntegreerd zullen worden in een nieuw totaalconcept van elektroni-

sche, elektrotechnische en telecommunicatiefaciliteiten. Een belangrijke aanzet hiertoe is gegeven door de recente ontwikkelingen in de automatiserings-industrie met haar kantoor- en produktie-automatisering.

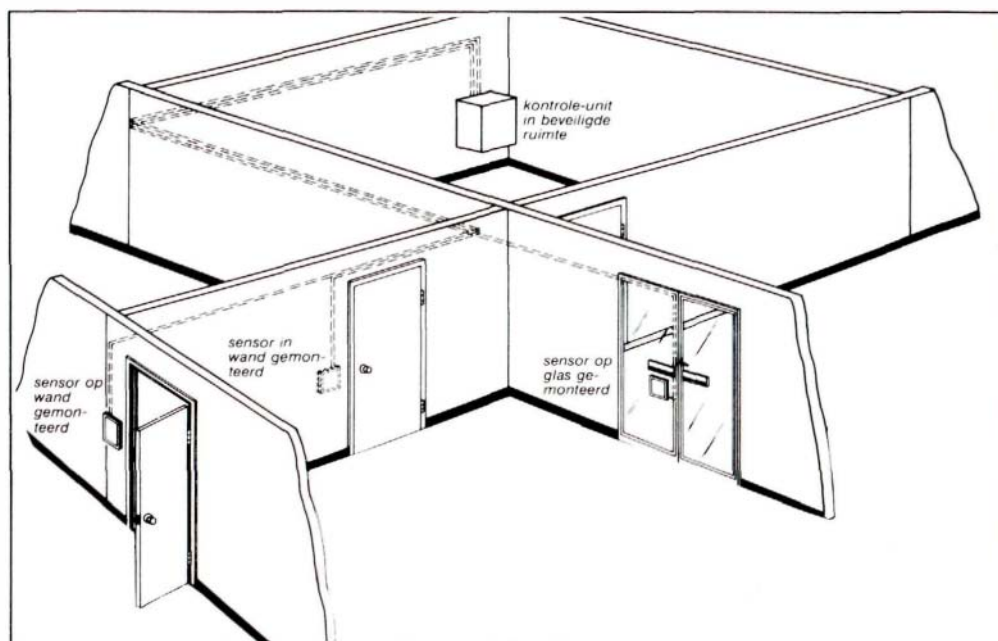
Op uitvoeringstechnisch terrein betekenen deze ontwikkelingen een integratie van alle verschillende netwerken die nu nog gebruikt worden in één groot gebouwenbeheersysteem. Eén universele informatiedrager door het gehele gebouw waarop alle subsystemen kunnen worden aangesloten; dus ook de beveiligingssy-
stemen.

Het is niet zo dat dit alles van vandaag op morgen zal worden gerealiseerd, maar ontwerptechnisch dient er alvast rekening met dit toekomstbeeld te worden gehouden.

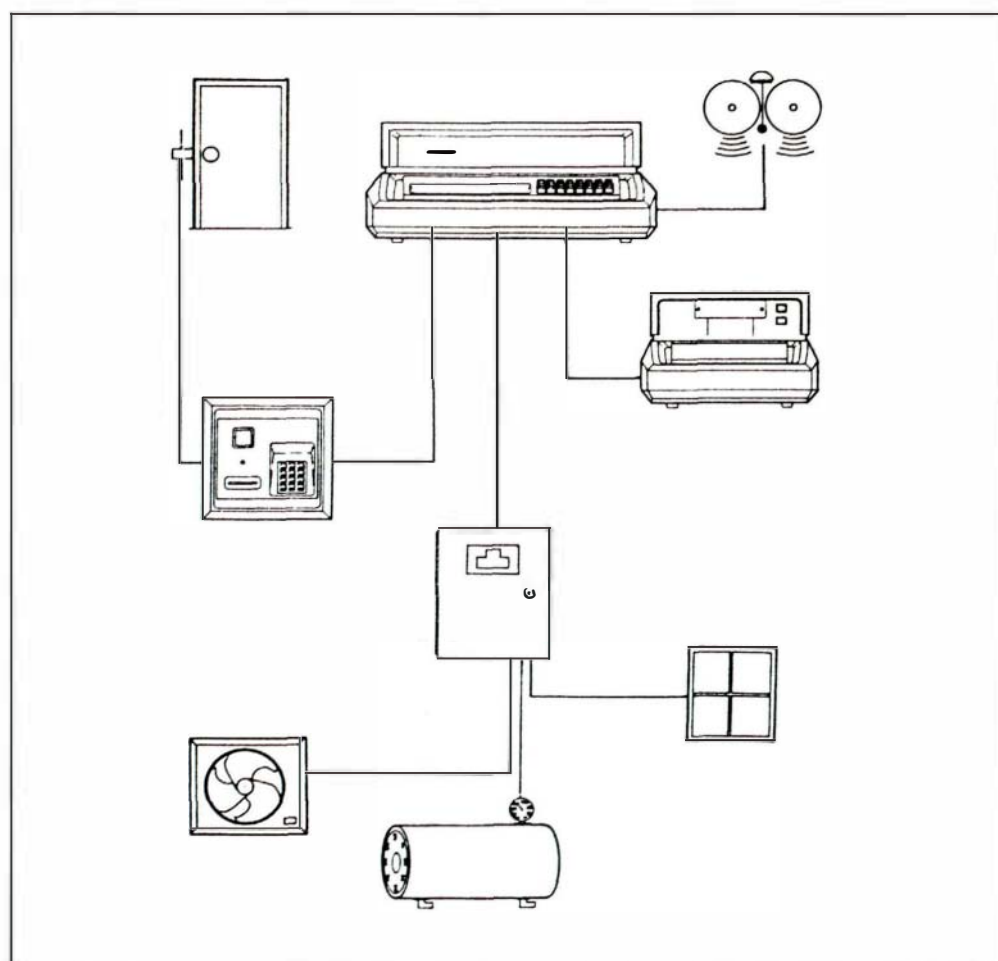


'Security centre'

Typisch voorbeeld van een klein systeem, waarbij de entree en twee belangrijke binnendeuren zijn beveiligd



Schematisch voorbeeld van toegangscontrole opgenomen in een groter gebouwen-automatise-ringsysteem



ONTWERP

Zoals bij vele beveiligingszaken het geval is wordt het effect van een compleet toegangscontrolesysteem in hoge mate bepaald door een goed ontwerp, waarin veel aandacht zal moeten worden besteed aan vier belangrijke factoren:

- mens en organisatie;
- het identificatiemiddel (de 'kaart');
- de kaartlezer;
- het deurconcept.

Het aantal variabelen in deze factoren is groot en eerst na een goed interview met de toekomstige gebruiker vooraf en een daarvan afgeleid programma van eisen kan tot een definitief ontwerp en een keuze van de produkten worden overgegaan. Het is verstandig in die fase gebruik te maken van de diensten van ervaren specialisten in dit vakgebied.

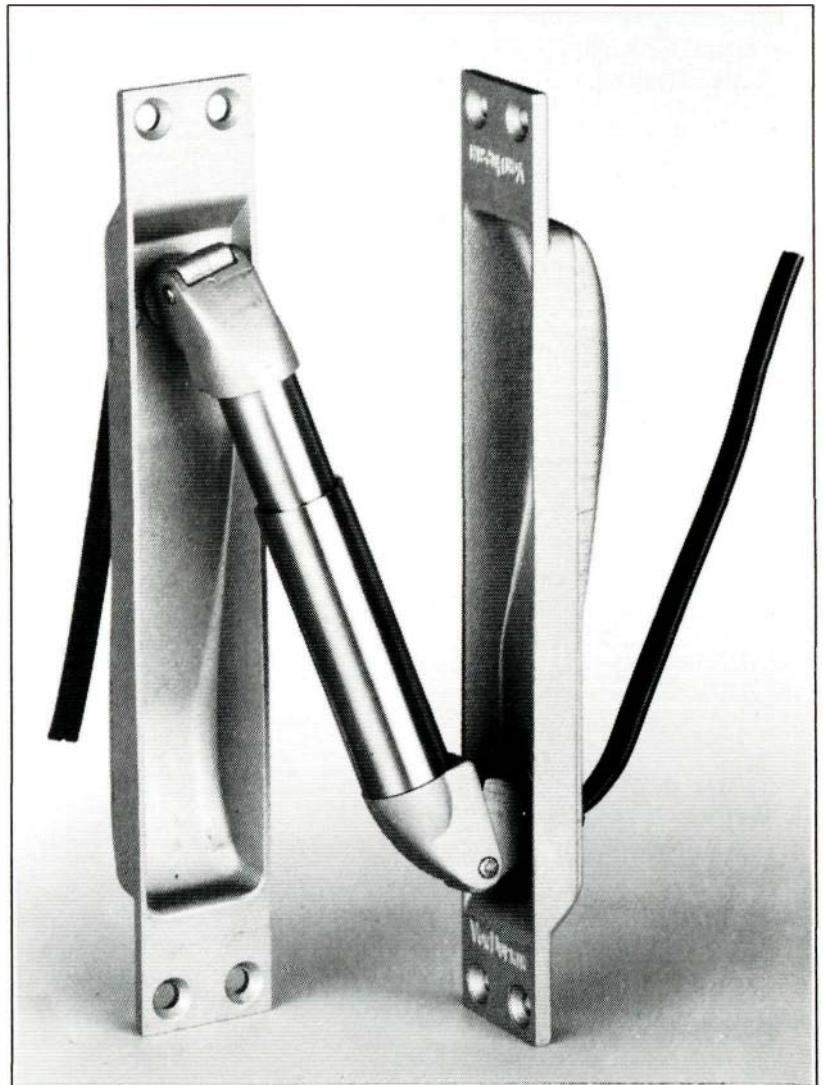
De specialist zal daarbij onder meer de volgende uitgangspunten hanteren:

Een goed toegangscontrolesysteem

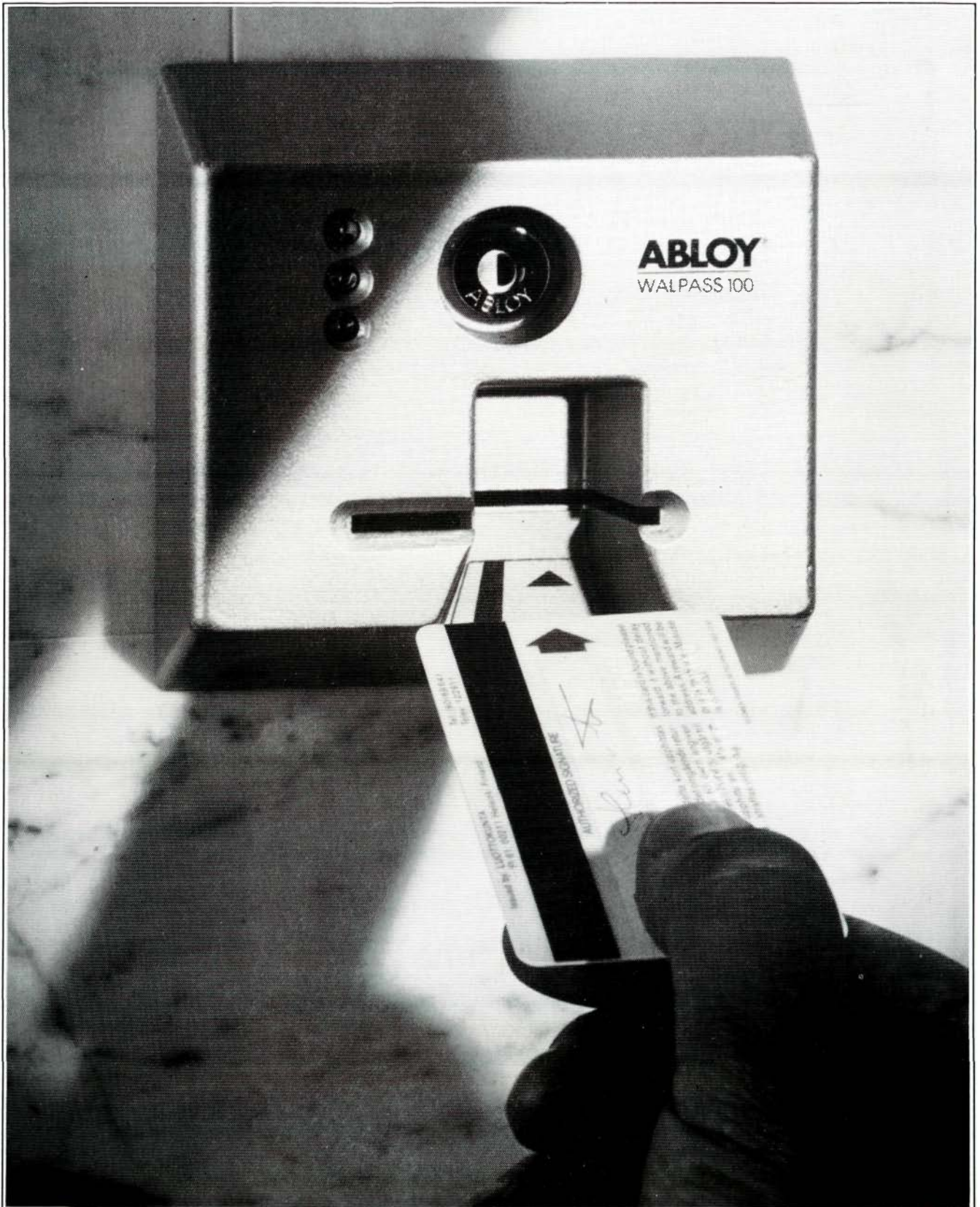
- past in het bedrijf;
- is eenvoudig te bedienen;
- hindert de gebruiker zo min mogelijk;
- is modulair van opzet;
- kan worden uitgebreid;
- biedt de mogelijkheid van registratie;
- kan snel inspelen op veranderingen in de organisatie;
- verhoogt de flexibiliteit van de beveiliging;
- verhoogt de mate van veiligheid en beveiliging.

Nadruk op bouwkundige details

In de praktijk blijkt met toegangscontrolesystemen wel eens wat mis te gaan door een slecht ontwerp en/of een slechte uitvoering van de elektronica. Een groot deel van de storingen in de praktijk komt evenwel voor rekening van de slecht ontworpen en/of uitgevoerde *bouwkundige details*, reden waarom hieraan in de volgende hoofdstukken uitgebreid aandacht wordt besteed.



*Bouwkundig detail:
Kabeldoorvoer aan
scharnierzijde van een
deur*



Wanneer de toegangscontrole over een langere periode storingsvrij moet functioneren (en waar bestaat deze wens niet?), moeten vooral de *bouwkundige details* zeer goed zijn uitgevoerd. Met het begrip 'bouwkundig detail' wordt hier in principe al datgene bedoeld wat niet direct aange-merkt kan worden als 'de elektronica' van toegangscontrolesystemen. Dit betreft dan niet alleen de componenten zoals deuren, (elektrisch bedien- de) sloten en sluitplaten, deurdrangers, behuizingen van bedieningspane- len en verdere apparatuur, maar ook de bevestiging daarvan, sparingen, doorvoeren van kabels enz. Komt er ondanks het feit dat alle denkbare zorg aan het systeem is besteed toch nog een storing voor, dan moet het systeem zodanig van opzet zijn dat een mechanische overname van essen- tiële functies mogelijk is. Een noodstroomvoorziening moet aanwezig zijn om enkele uren stroomuitval te kunnen opvangen.

DE KAARTLEZER

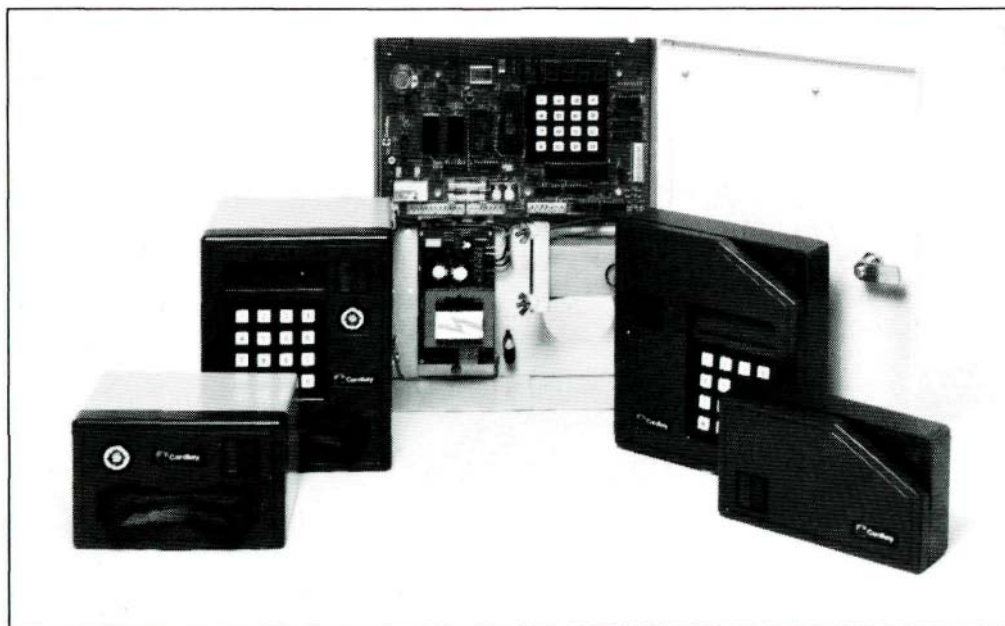
De kaartlezer — vooral als die buiten het beveiligd gebied is geplaatst — moet vol- doende bestand zijn tegen vandalisme, vocht, stof, statische elektriciteit enz. Grofweg vallen er drie 'modellen' te on- derscheiden:

- de kaartlezer waarbij de kaart in een sleuf (ter breedte van de kaart) gesto- ken moet worden;
- de kaartlezer waarbij de kaart voor een deel door een sleuf getrokken of geduwd moet worden;

- de kaartlezer waarbij de kaart alleen maar in de buurt van de kaartlezer gehouden hoeft te worden.

Deze modellen zijn verkrijgbaar in op- bouw- en inbouwuitvoering, mét en zon- der toetsenpaneeltje waarop een PIN- code kan worden ingetoetst.

Uit esthetisch oogpunt, maar nog meer vanwege het ontbreken van mogelijkhe- den tot (opzettelijke) beschadiging, ver- dient de inbouwuitvoering altijd de voor- keur. Het model zonder sleuf biedt daarnaast nog het grote voordeel dat dit niet opzettelijk onbruikbaar kan worden



Kaartlezers in diverse uitvoeringen

gemaakt door kauwgom, paperclips enz. Het is een volkomen gladde rechthoekige plaat met een oppervlak van enkele vierkante decimeters met een dikte van ongeveer een centimeter. Deze plaat kan desnoods onzichtbaar onder bijvoorbeeld een vinyl wandbekleding worden weggewerkt. De kaartlezers met een toetsenpaneeltje moeten zódanig worden geprojecteerd dat 'meekijken' bij het intoetsen van een PIN-code niet mogelijk is.

HET DEURCONCEPT

Aan de entreepartij van een kantoorgebouw worden nogal wat eisen gesteld. In de eerste plaats komt de vormgeving; de entree is immers het 'visitekaartje' van het gebouw en de daarin gevestigde onderneming(en). Daarnaast zijn er de eisen van gebruiksvriendelijkheid, gebruikscapaciteit, het toegankelijk zijn voor invaliden, tochtwering enz. en in het kader van dit rapport: een zodanige layout van de entreepartij dat inbraakwering en toegangscontrole mogelijk zijn. Voor

de ontwerper brengen deze bijzondere eisen met zich mee dat hij naast voldoende constructief inzicht nogal wat specifieke kennis en ervaringen op het gebied van beveiligde entreepartijen moet hebben opgedaan, wil althans zijn ontwerp in een goed functionerende entree resulteren. Bij twijfel is het derhalve raadzaam al in een zovroeg mogelijk stadium een specialist op het gebied van entreepartijen in de arm te nemen.

In dit hoofdstuk zullen de meest voorkomende (buiten)deursituaties van hoofd- en andere in- en uitgangen van kantoorgebouwen worden behandeld. Voor die kantoren waar over een eigen afsluitbaar terrein kan worden beschikt en waarbij terreinbeveiliging wordt toegepast, worden de poorten in hoofdstuk 11 behandeld.

DEUREN IN KANTOREN

Voor kantoren zal de keuze uit het grote assortiment van deuren doorgaans beperkt blijven tot:

Entree-partij



Hoofd-entreepartij:

- enkel- of dubbelbladige draaideur in aluminium met glas of volglas;
- enkel- of dubbelbladige horizontaal schuivende deur in aluminium met glas;
- kruisvleugeldeur (tourniquet) in aluminium met glas.

Overige in- en uitgangen:

- enkel- of dubbelbladige draaideur in hout, aluminium of staal (eventueel met glas);
- in verticale richting schuivende en/of kantelende deur uitgevoerd in aluminium (eventueel met glas) voor afdelingen in kantoren zoals 'expeditie' of grotere technische ruimten.

In de hoofd-entreepartijen worden veelal combinaties van de drie genoemde uitvoeringen toegepast, in toenemende mate met een automatische elektrische bediening.

De entreepartijen moeten enerzijds passen in het eisenpakket voor het weren van inbraak en vandalisme en anderzijds moeten ze aan de eisen kunnen voldoen die voor de toegangscontrole noodzakelijk zijn. Details over *inbraak- en vandalismerende* deuren en kozijnen die hier van toepassing zijn, worden in de serie Beveiliging van gebouwen in de delen 1, 2 en 3 behandeld, onder meer:

- deel 1, hoofdstuk 3 onder: Keuzeaspecten van kozijnen, ramen en deuren (hout, metaal en kunststof) (inbraak);
- deel 2, hoofdstuk 5 onder: De entree, en onder: Entreedcuren (vandalisme);
- deel 3, hoofdstuk 5 onder: De pui (inbraak en vandalisme)

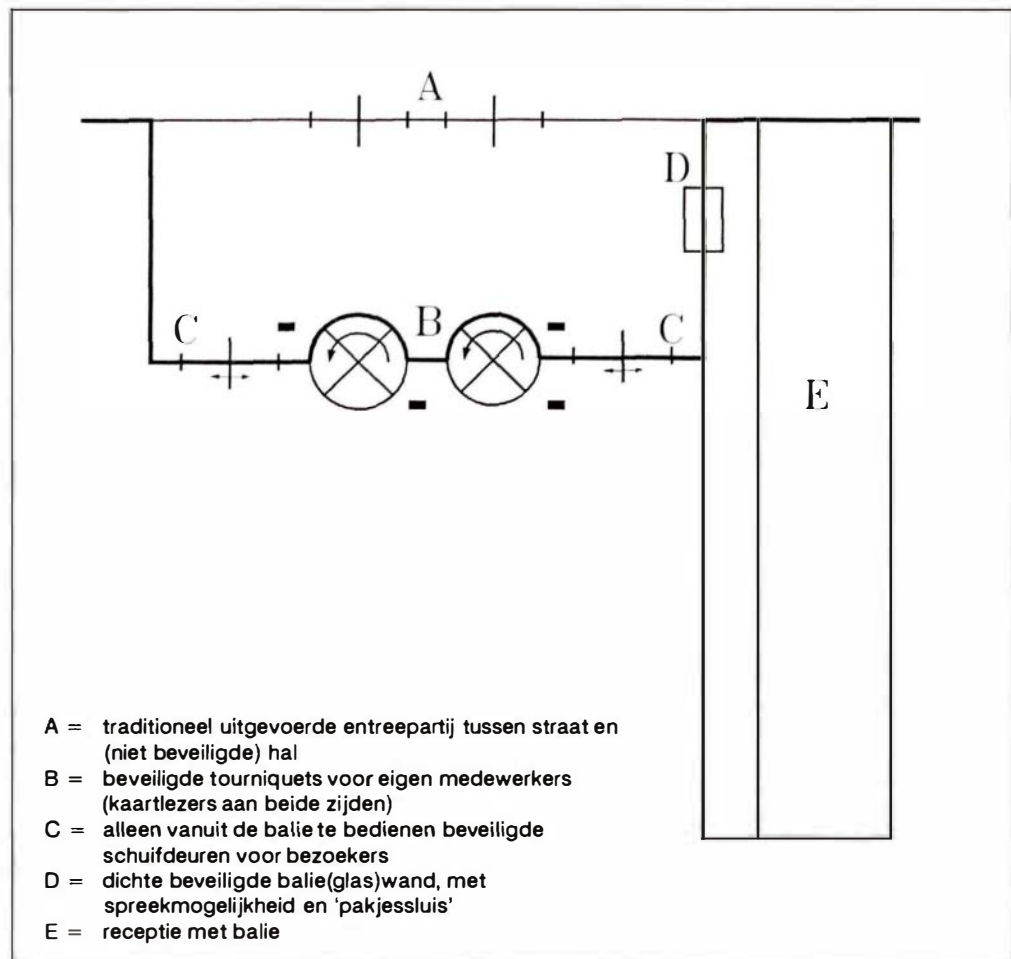
Met name de Normen, NPR's en andere referenties die geheel of gedeeltelijk ook voor kantoren van toepassing moeten of kunnen worden verklaard, komen in voornoemde delen uitvoerig aan de orde.

Wanneer we na al deze verwijzingen weer terugkomen bij het onderwerp *toegangsbeveiliging*, zien we dat bij bevoegd gebruik van een traditionele draai- of schuif-

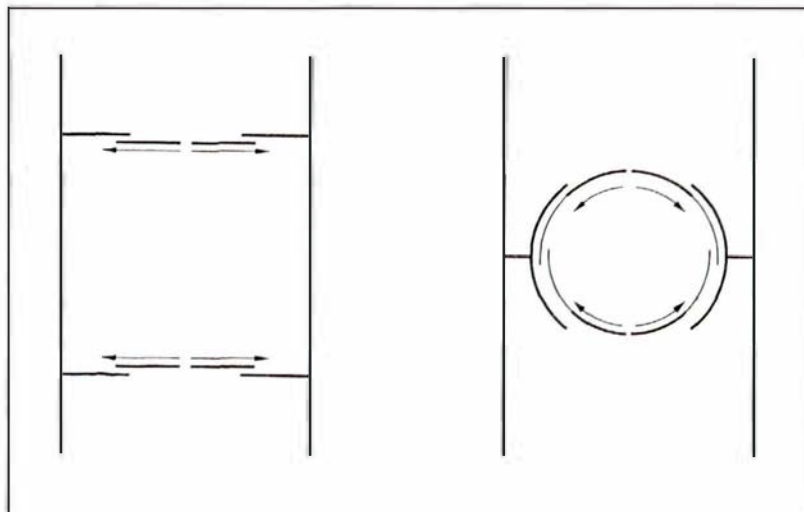
deur steeds gedurende circa vijf tot vijftien seconden een 'gat' in de beveiliging ontstaat, omdat na het passeren van de bevoegde gemakkelijk één of meerdere onbevoegde personen 'mee naar binnen kunnen glippen'. Een andere mogelijkheid van 'sabotage' is om, nèt voordat de deur na gebruik terugvalt in het slot, deze tegen te houden. Worden twee deuren gebruikt die zodanig zijn geschakeld dat de ene deur alleen kan worden geopend nadat de andere deur is gesloten (er is dan sprake van een zogenaamde 'interlocked-sluis') dan is de kans op het 'meeglippen' natuurlijk aanzienlijk kleiner. Is de ruimte tussen de twee deuren evenwel te groot, dan is het nog steeds mogelijk dat met een toegangsverlening aan één persoon aan meerdere personen gelijktijdig toegang wordt verleend. Wanneer de ruimte tussen de beide deuren zodanig wordt uitgevoerd dat zich slechts één persoon in deze sluis kan bevinden, dan is er sprake van een individuele toegangscontrole.

Een nadeel van sluizen is dat deze nogal wat vloeroppervlak in beslag nemen en dat het passeren ervan veel tijd kost, zodat de capaciteit laag is. Toegangen waarvan door een groot aantal bevoegden in korte tijd gebruik moet worden gemaakt, kunnen het best worden voorzien van één of meerdere beveiligde tourniquets (kruisvleugeldeuren), waarin dan meestal slagwerend glas wordt toegepast. De kwadranten van de tourniquets zijn voor dit doel zodanig verkleind dat zich hierin gelijktijdig slechts één persoon kan bevinden. Bovendien worden bij dit soort uitvoeringen voorzieningen getroffen waardoor het bijvoorbeeld niet mogelijk is dat een bevoegde de tourniquet in de ene richting gebruikt (bijvoorbeeld het gebouw uit), terwijl een onbevoegde in een ander kwadrant van de deur gelijktijdig meeloopt in tegenovergestelde richting (het gebouw in). Met behulp van allerlei soorten detectiemiddelen kunnen in geval van ongeautoriseerd gebruik diverse blokkades worden gerealiseerd.

Een beveiligde tourniquet oogt bepaald niet vriendelijk en op plaatsen waar veel bezoekers komen is dit vaak ongewenst.

Beveiligde entree-situaties

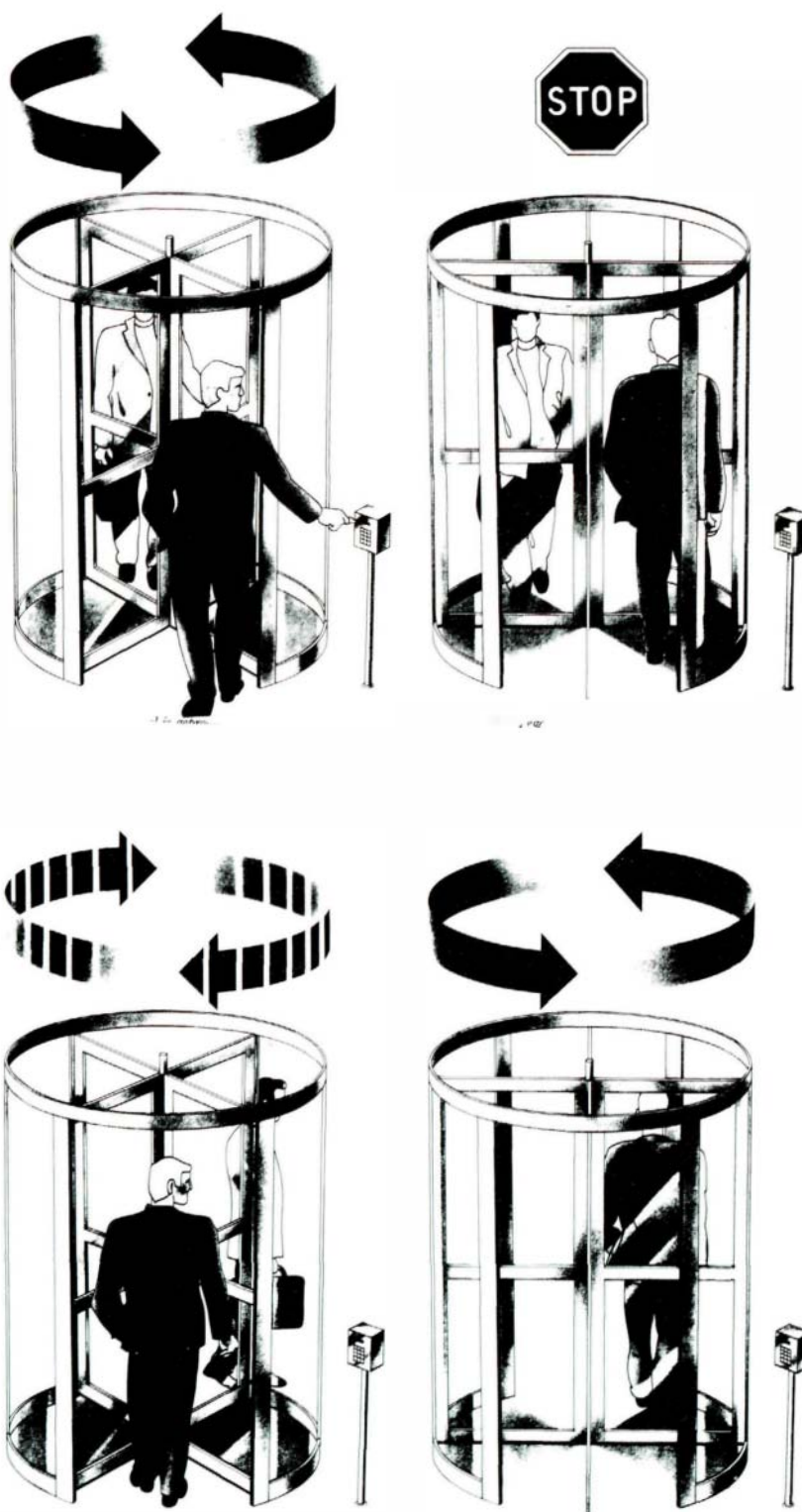
Omdat zich bij deze toegangen juist in verband met het bezoek veelal beveiligingsbeambten of receptionisten bevinden, kan in die gevallen het toepassen van

Sluizen en tourniquets

zogenaamde 'drietanden' een (tijdelijke) oplossing zijn. Bevoegden kunnen met hun kaart de drietand ontgrendelen, terwijl bezoekers zich automatisch melden bij de bewakers of de receptie. Er dient natuurlijk wel een continu toezicht te zijn bij dergelijke oplossingen omdat de fysieke belemmering maar zeer beperkt is. De drietand dient alleen als hulpmiddel voor de controle door beveiligingsbeambten en/of receptiepersoneel.

Speciale 'sluisdeuren'

Al eerder werd gezegd dat de zogenaamde interlocked sluis (twee van elkaar afhankelijk geschakelde deuren) veel vloeroppervlak in beslag neemt. Voor enkele speciale sluisdeuren geldt dit bezwaar aanzienlijk minder.

Beveiligde touniquet**Situatie links/boven:**

Deze veiligheids-carroussel is geprogrammeerd om zowel het binnengaan als het uitgaan te controleren. Iemand die naar buiten wenst te gaan stelt de deur in werking met de sleutelkaart of middels het toetsenbord/codeschakelaar.

Een niet-bevoegd persoon is op weg vanuit tegenovergestelde richting.

Situatie rechts/boven:

Zodra de onbevoegde persoon de controlezone binnenkomt stopt de deur.

Hetzelfde zou zijn gebeurd indien een onbevoegde persoon zou hebben getracht naar buiten te sluipen achter de bevoegde persoon aan. De positie van de deur geeft noch toegang naar binnen, noch naar buiten.

Situatie links/onder:

Na het stoppen draait de deur automatisch terug naar de start-positie. Degene die op weg naar buiten is, zowel als de onbevoegde persoon, dienen de carroussel te verlaten.

De terugdraai-functie voorkomt dat iemand in de carroussel opgesloten blijft.

Situatie rechts/onder:

Zodra de onbevoegde persoon de controlezone verlaten heeft, hervat de deur de normale draaiing automatisch en laat de onbevoegde persoon door. Indien een onbevoegde persoon een legitieme bezoeker is, moet men contact met de beveiligingsdienst opnemen om een tijdelijke bevoegdheid te krijgen om naar binnen of naar buiten te gaan.

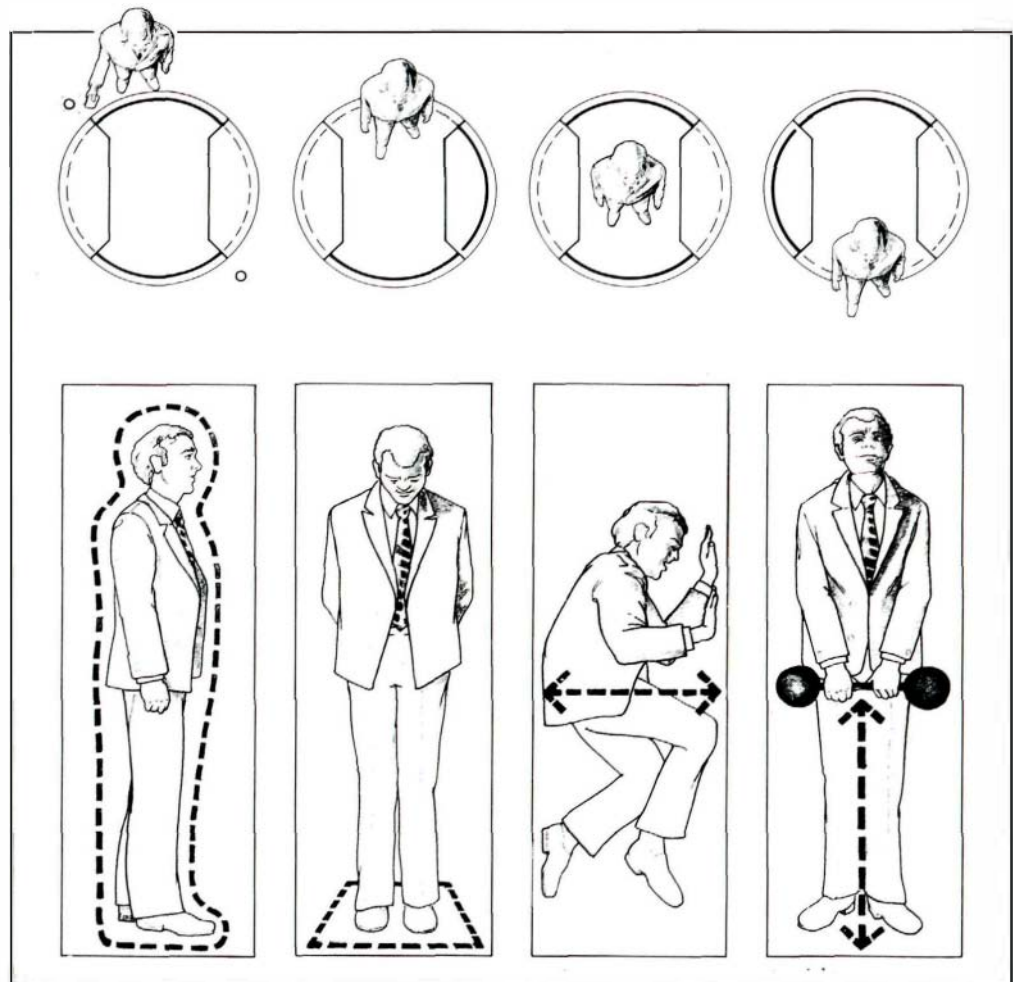
Voorbeeld van speciale sluisdeur: 'circle-lock'

Boven, van links naar rechts:

- Passant meldt zich aan. Via de kaartlezer opent de eerste deur.
- Passant stelt zich op in het midden van de sluis. De eerste deur blijft open en de tweede gesloten.
- Alle sensoren controleren thans.
- Alle informatie is in overeenstemming, de eerste deur sluit en de tweede opent. De passant treedt naar buiten en meteen sluit de tweede deur. De circle-lock heeft een capaciteit van gemiddeld 5 à 6 personen per minuut, afhankelijk van het type kaartsysteem.

Onder, van links naar rechts:

- 'Vorm'
- Sensor controleert vorm en volume. Doorgang wordt geblokkeerd zodra twee personen zich opstellen.
- 'Positie'
- Sensor controleert positie van de voeten. Het beschikbare registratie-oppervlak biedt plaats aan één paar voeten.
- 'Inklemmen'
- Sensor controleert de stand van de wanden. Zodra uitbuijing plaatsvindt, blijft de doorgang geblokkeerd.
- 'Gewicht'
- Sensor controleert gewicht van de passant. Hierbij wordt het gewicht van de totale kooi betrokken.



Sabotage

Het introduceren van met name geautomatiseerde toegangscontrolesystemen in bedrijven is vaak een ingrijpende gebeurtenis.

Dergelijke systemen slagen alleen wanneer deze logisch van opzet zijn, in voldoende mate organisatorisch worden begeleid en er 'streng' wordt toegezien op een juist en consequent gebruik. Het handhaven van sluipwegen, hetzij in fysieke hetzij in procedurele zin, werkt demotiverend voor de gebruikers. Van groot belang is ook dat dergelijke systemen door de directie van een bedrijf worden geaccepteerd en ondersteund. Een beveiligingsbeambte die geen steun ondervindt bij zijn leiding, zal snel de teugels laten vieren. Ook slechte bezoekersregelingen zijn er veelal de oorzaak van dat een op

zichzelf goed toegangsverleningssysteem gemakkelijk wordt omzeild.

De gebruiksvriendelijkheid is verder een belangrijk aandachtspunt. Veelal gaat een stijgend beveiligingsniveau gepaard met een verminderde mate van gebruiksvriendelijkheid. Toegangsbeveiliging is meestal strijdig met de eisen voor ontvluchting bij brand of andere calamiteiten. Ook intern transport vergt doorgaans maatregelen die een consequent toepassen van toegangscontrole negatief beïnvloeden.

Wanneer aan de hiervoor genoemde aandachtspunten geen of onvoldoende aandacht wordt besteed is het negatieve eindresultaat met de daarbij behorende irritaties voorspelbaar. Er is dan veel geld uitgegeven aan een systeem dat het beoogde beveiligingsniveau niet haalt en/of goedwillende bevoegde gebruikers voelen zich door het systeem geplaagd, mede

omdat kwaadwillenden het systeem saboteren.

Overige in- en uitgangen

Tot nu toe is in het voorgaande alleen aandacht gegeven aan deuren in entreepartijen. Het behandelde kan betrekking hebben op de hoofd-entree van een kantoorgebouw, maar ook op de entreepartij die toegang geeft tot een beveiligde afdeling of gebied in een kantoor.

De (buiten)deuren die zijn opgenomen in een vluchtweg zijn behandeld in hoofdstuk 7 onder: Daken en vluchtwegen, terwijl de deuren voor speciale 'compartimenten' zoals kluis- en archiefruimten zijn behandeld in hoofdstuk 8: Compartimenteren.

Wat resteert met betrekking tot de beveiliging van kantoren, zijn de overige binnen- en buitendeuren, zoals:

- aparte (buiten)deuren voor personeel, leveranciers/onderhoudsdiensten enz. Dit zullen vrijwel altijd op de gebruikelijke wijze uitgevoerde enkele of dubbele glas- of 'volglas'-deuren zijn.
- één of meerdere grote buitendeuren voor ruimten met bijvoorbeeld afvalcontainers, garage, en dergelijke.
- binnendeuren voor speciale ruimten, zoals voor opslag van kantoorbenodigdheden, technische ruimten, ruimten voor schoonmaakdiensten, enz. Dit zullen veelal blinde deuren zijn.

Afhankelijk van de waarde van de betreffende deuren in het beveiligingsplan zullen deze meer of minder inbraakwerend dienen te worden uitgevoerd, en tevens meer of minder in de toegangsbeveiliging moeten worden betrokken.

Blinde deuren kunnen het best in massief triplex ('multiplex') worden uitgevoerd, of in staal met hang- en sluitwerk volgens NEN 5088/89 (extra zwaar ***).

Bij glasdeuren zal afhankelijk van de situatie meer of minder slagwerend glas moeten worden toegepast. Van belang is daarbij onder meer dat het glas voldoende diep in de sponning wordt opgelegd en in binnenbeglazing wordt uitgevoerd (zie



deel 3, hoofdstuk 5 onder Het glas). Volglasdeuren kunnen ook uitstekend inbraak- en zelfs kogelwerend worden uitgevoerd. Ze zijn dan uiteraard niet van gehard glas gemaakt. Dit type deuren mist een kader, maar heeft aan boven- en onderzijde een horizontaal aangebracht verdiept U-profiel ('dorpel') waarin het speciale slagwerende glas is opgesloten. Aan de sluitzijde zijn deze profielen met een lange verticaal lopende greep aan elkaar gekoppeld. In genoemd onder- en bovenprofiel bevinden zich dan tevens de scharnierpunten (aan de onderzijde in een vloerdeurveer of vloerpot), alsmede de (eventueel elektrisch te bedienen) sloten. In plaats van een onder- en bovenslot kan een slot ook op de gebruikelijke krukhooft worden aangebracht. In dat geval wordt op die hoogte een horizontale metalen band van 10 à 20 cm. hoog rond het glaspakket aangebracht, waarin het slot is opgenomen.

De grotere bedrijfsdeuren voor containerruimten en dergelijke zijn in speciale inbraakwerende uitvoeringen in de hande. Er kan in veel gevallen natuurlijk ook een rolluik worden toegepast. Belangrijk is dat de erachter liggende — vaak openstaande — ruimte geheel blind is en maar één blinde verbinding deur met het kantoorgedeelte heeft. Deze (vaak dubbele) draaideur moet beveiligingstechnisch als buitendeur worden beschouwd en dienovereenkomstig inbraakwerend worden gedetailleerd. Om meerdere redenen is het gewenst dat in dit soort ruimten ook branddetectie en/of een sprinklerinstallatie wordt toegepast.

Draairichting

In de communicatie over draairichtingen van ramen en deuren gaat nogal eens iets mis, hetgeen tot onbruikbare (beveiligings)produkten op de bouw kan leiden. Op de volgende pagina zijn zowel de Nederlandse, de Engelse en de Duitse benaming aangegeven voor insteekdeur- en loopsloten, alswel de internationale situatie-symbolen voor de draairichtingen.

Automatische deuren en aandrijvingen

In toenemende mate worden ook in kantoorgebouwen automatische deuren toegepast die worden aangestuurd door een personendetector (passief-actief infrarood- of radar-detector), een drukknop of een toegangscontrolesysteem. Ook kunnen de verschillende aansturingen wisselend worden gebruikt door toepassing van een keuzeschakelaar. In toegangsbeveiligde gebieden wordt de personendetector natuurlijk niet toegepast, hooguit voor het verlaten van het beveiligde gebied.

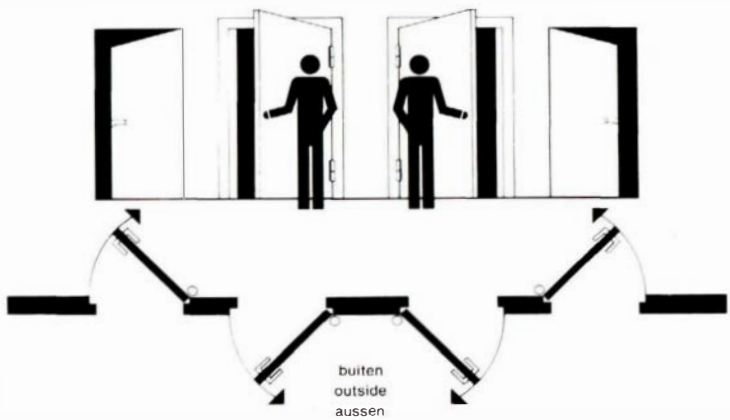
De meest voorkomende typen automatische deuren zijn uitgevoerd als schuifdeur: één- of tweezijdig schuivend, al dan niet telescopisch. Dan zijn er verder nog de gebruikelijke draaideuren die automatisch kunnen worden bediend, en er zijn zelfs (vaag op een tourniquet lijkende) ronde automatische schuifdeuren (zie ook hoofdstuk 10 onder Speciale sluisdeuren)

De aandrijving (elektromechanisch of hydraulisch) voor de deurvleugels wordt in de meeste gevallen gemonteerd op de draagconstructie of het kalf. Er zijn hiervoor speciale uitvoeringen met een zelfdragend kalf.

Bij de gebruikelijke automatische schuifdeuren hangen de deurvleugels aan het loopwerk (loopwagen) met enkele of dubbele loopwielen, dit afhankelijk van het gewicht. Bij snel openende deuren (0,5–1 m/sec. per deurvleugel) is bij de toepassing van de gebruikelijke technieken het maximum-deurvleugelgewicht ca. 250 kg. Gaat het openen en sluiten langzamer (dus geen entree waar veel personen door moeten), dan mag het gewicht meer zijn, wel tot 3000 kg, zoals bij stralingsvrije deuren. De deurvleugelophanging en het doorgaans smalle kader waarin het glas gevat is, brengen met zich mee dat de gebruikelijke automatische schuifdeur maar beperkt inbraakwerend is.

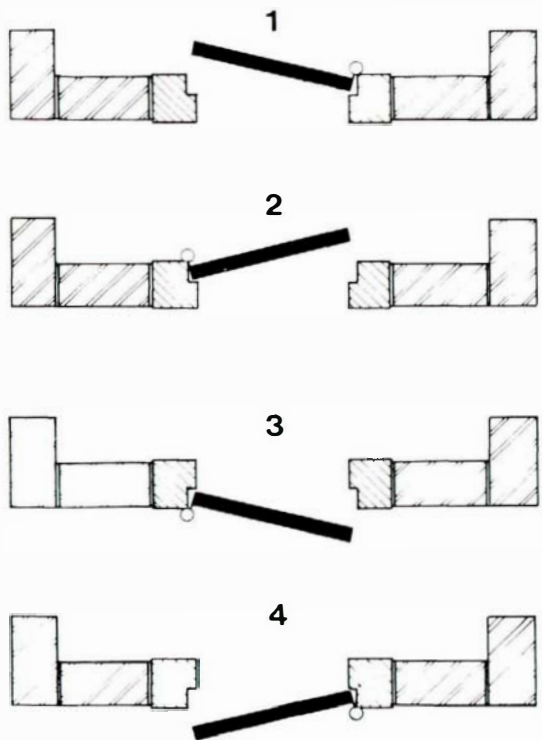
Wordt een dergelijke deur ook als buitendeur in het kantoorgebouw toegepast dan zal voor een inbraakwerende uitvoering moeten worden gekozen, zoals we die ook zien toegepast bij banken en supermark-

INSTEELK DEUR- EN LOOPSLOTEN
MORTICE LOCKS AND LATCHES • EINSTECK TURSCHLOSSER



NL	RECHTS SLOT	LINKS SLOT	RECHTS SLOT	LINKS SLOT
GB	LEFT HAND	RIGHT HAND	LEFT HAND	RIGHT HAND
D	RECHTSEINWARTS (DIN LINKS)	RECHTSAUSWARTS (DIN RECHTS)	LINKSAUSWARTS (DIN LINKS)	LINKSEINWARTS (DIN RECHTS)

INTERNATIONALE SITUATIE-SYMBOLEN
VOOR DE DRAAIRICHTINGEN VAN DEUREN EN RAMEN



ten. Deze deuren onderscheiden zich van de standaarduitvoering door het dikkere (zwaardere) slagwerende glas, brede stalen/aluminium kaders met één of meerdere tussenregels. Na sluitingstijd kunnen deze deuren met meerpuntsvergrendelingen worden afgesloten. Dat kan bijvoorbeeld een zwenkhaakslot met boven- en eventueel ondergrendel zijn. Eventueel kunnen elektrisch bedienbare sloten worden toegepast.

Het moet uitgesloten zijn, dat automatische deuren via de kast van de aandrijving (handslinger voor noodsituaties, bekabeling en dergelijke) aan de buitenzijde kunnen worden beïnvloed.

SPECIAAL HANG- EN SLUITWERK

In hoofdstuk 9, Toegangscontrole, is de functie van een aantal toegangscontrolesystemen uiteengezet. In deze paragraaf wordt nader ingegaan op de details en toebehoren van dat soort systemen.

Sloten en sluitsystemen

Sloten kunnen we onderscheiden in slot-systemen (bontebaard-, klavier- en cilinderslot) en uitvoeringen waarin het slot-systeem is ondergebracht (insteekslot, oplegslot, hangslot enz.). Het slotmechanisme dient er slechts toe dat met de juiste sleutel de schoot kan worden bewogen. Het bontebaardslot (het oude keukenbuitendeurslot) is zeer onbetrouwbaar op dit punt en heeft dan ook qua inbraakbeveiliging geen enkele waarde. Een klavierslot kan zeer vergaand bestand zijn tegen manipulaties via het sleutelgat, en het kan ook in zijn totaliteit inbraakveilig zijn. Toch word het als bouwslot steeds minder toegepast, onder andere vanwege de kostprijs.

In praktische zin resteren derhalve als bouwslot de cilindersloten. Een groot voordeel bij dit type slot is dat de cilinders gemakkelijk en relatief goedkoop verwisseld kunnen worden. De cilinders zijn in verschillende vormen en afmetingen verkrijgbaar, maar voor het merendeel wor-

den de laatste tijd de zogenaamde (Euro)profielcilinders (volgens DIN) toegepast. Een ander voordeel is, dat deze profielcilinder gemakkelijker aansluit op het grote aanbod van het bij sloten behorende beslag. Gemakkelijker althans dan andere cilindervormen zoals ovaal- en rondcilinders. Inbraakveilige sloten en cilinders moeten voldoen aan: NEN 5089: Inbraakveiligheid van gebouwen; Inbraakwerend hang- en sluitwerk; Eisen en beproevingsmethoden.

Met sloten kunnen we op relatief eenvoudige wijze toegangen beveiligen. Met cilindersloten waarbij de cilinders in een sluitplan zijn opgenomen, kunnen we van een vorm van toegangscontrolesysteem spreken.

Een sluit- of sluitingssysteem – ook wel hoofdsleutelinrichting genoemd – is een geheel van profielcilinders, waarvan de organisatorische opbouw door de opdrachtgevers zo wordt samengesteld, dat een persoon slechts toegang heeft tot die ruimten waar hij door het sluitingssysteem wordt toegelaten. Zo kan bijvoorbeeld in een groot kantoorgebouw de directie met haar hoofdsleutel overal naar binnen, maar naarmate men daalt op de hiërarchische ladder verkleinen de toegangsmogelijkheden van zijn sleutel. In een hoofdsleutelinrichting kunnen eventueel ook de cilinders van hangsloten, meubelsloten, knopsloten, brievenbussen enz. worden opgenomen.

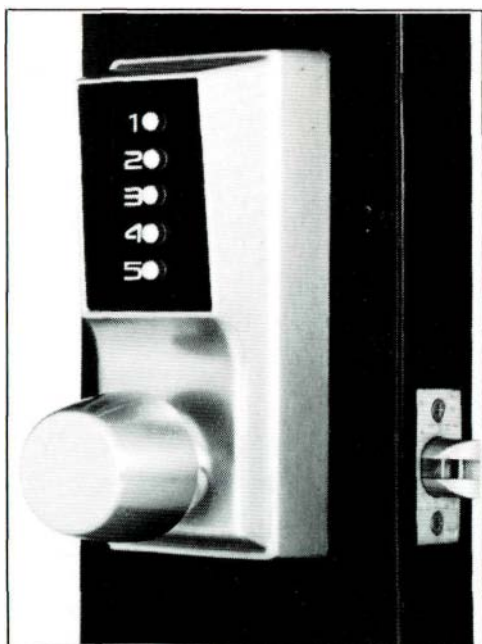
De behandelde sloten en sluitsystemen staan op pag. 108 en 109 beschreven en schematisch weergegeven.

Het sluitplan is de basis van iedere bestelling en tevens het werkdokument om het sleutelsysteem op te kunnen bouwen. In het sluitplan worden de organisatorische opbouw en alle bijzonderheden omtrent de cilinders en sleutels in de vorm van een schema vastgelegd. De opdrachtgever krijgt van de slotenfabrikant een kopie van dit sluitplan. Iedere cilinder draagt een codenummer dat overeenkomt met het codenummer op het sluitplan.

Mechanische codesloten

Een mechanisch codeslot is een slottype waarbij men in plaats van een sleutel een code invoert. Er zijn verschillende uitvoeringen. We schenken hier aandacht aan een veel voorkomend type. De (schootbediende) knop aan de binnenzijde is altijd vrij om de deur te openen, terwijl de buitenknop alleen kan worden bediend als de juiste code is ingetoetst. Het is erg belangrijk om de cijfercombinatie in de juiste configuratie in te toetsen. Doet men dit niet dan zal het resultaat een gesloten deur zijn. De codenummers kunnen steeds worden gewijzigd, zonder toevoeging of vervanging van onderdelen, en bestaan uit een willekeurig aantal codetoetsen, enkel of tegelijk in combinatie te bedienen. Na het sluiten van de deuren is de buitenknop automatisch weer buiten werking gesteld.

Er zijn ook uitvoeringen met een verwisselbare cilinder in de buitenknop, zodat men ook door middel van een sleutel toegang kan krijgen. Tevens zijn er uitvoeringen waarbij het slot gedurende een bepaalde periode met een vrijzetknop buiten werking kan worden gesteld. Eventueel kan deze knop om beveiligingstechnische redenen als cilinder met sleutel



worden uitgevoerd.

De sloten kunnen doorgaans op alle voorkomende deurbladdikten van circa 35–57 mm worden geplaatst, en hebben doormaten van bijvoorbeeld 70–127 mm.

Elektrische deurgrendels

Elektrische deurgrendels worden toegepast voor het op afstand vergrendelen of ontgrendelen van beveiligde deuren, geheel onafhankelijk van een eventueel aanwezig deurslot. De grendel valt in de sluitplaat, de sluitpost of de sluitkom. Er zijn verschillende typen qua elektrische bediening: onder spanning ontgrendeld, of onder spanning vergrendeld, ofwel bij spanningsuitval blijft de vergrendelen in de laatst gekozen stand. Veelal is een micro-switch ingebouwd voor de stand van de vergrendelen ('dicht' of 'open'), en soms ook voor de signalering van het saboteren, of het losnemen van delen van de behuizing. Een aantal elektrische deurgrendels is zo uitgevoerd dat ze als smal-slot in metalen deuren met smalle profielen kunnen worden toegepast, maar ook in de kozijnstijl of in het kalf boven de deur. Het slot dient dan tevens als hoofdslot. Dit type sloten kan dan doorgaans ook nog met een cilinder worden bediend. De speciale 'beveiligingsuitvoeringen' voldoen doorgaans op het belangrijke onderdeel schoot ruim aan de in de NEN 5089 genoemde waarden voor zijdelingse druk. Bij toepassing in de deur is het van belang dat een zeer deugdelijke kabeldoorvoer aan de hangzijde wordt toegepast.

links:

Mechanisch codeslot

Elektrische deuopeners

Elektrische deuopeners worden gebruikt om een gesloten deur op afstand te ontgrendelen. Het meest voorkomende type deuopener is op de plaats van de sluitplaat of de sluitkom gemonteerd. De elektrische deuopener zorgt ervoor dat de uitstaande dag- of nachtschoot vrij komt te liggen in de sluitkom, zodat de deur kan worden geopend.

(naar pag. 110)

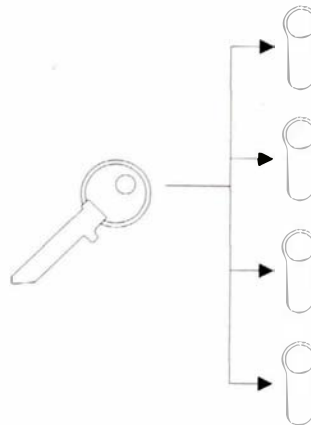
Behandelde sloten en sluitsystemen

De volgende sloten en sluitsystemen kunnen met cilinders worden opgebouwd:

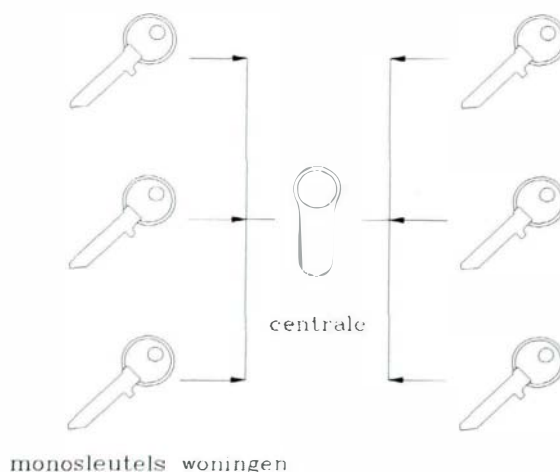
- A *Gelijksluitende cilinders:*
Meerdere cilinders kunnen met één sleutel worden bediend;
- B *Centraal-sluiting:*
Meerdere (mono)sleutels (toegang gevend tot een eigen ruimte) passen bijvoorbeeld ook op de centrale hoofdentree;
- C *Centraal-sluiting met hoofdsleutel:*
Als B, maar nu kan men met een hoofdsleutel ook in alle ruimten en de centrale hoofd-entree;
- D *Hoofdsleutelsysteem:*
Als C, zonder een centrale hoofd-entree;
- E *Generaal hoofdsleutelsysteem:*
Meerdere groepen met een hoofd- en sub-hoofdsleutelsysteem, waarbij een generale hoofdsleutel (GHS) op *alle* cilinders past.

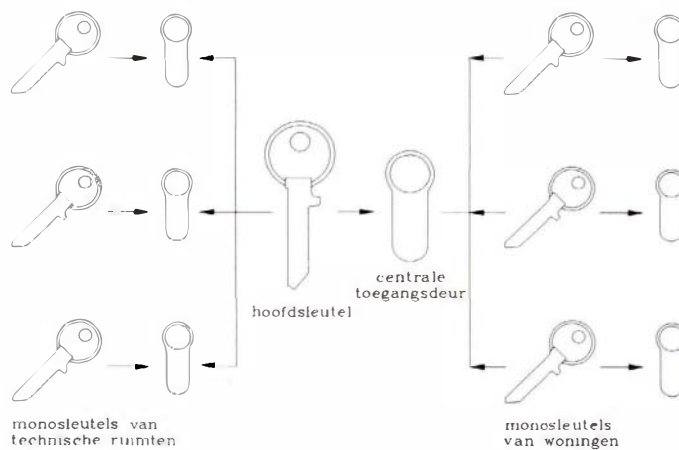
Met een generale sleutel en met hoofd- en sub-hoofdsleutels moet men natuurlijk zeer gecontroleerd omgaan. De illustraties geven de opbouw van voornoemde systemen weer.

Systeem A Gelijksluitende cilinders

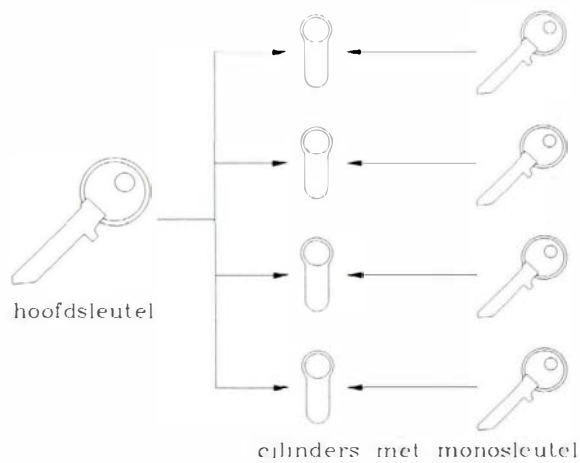


Systeem B Centraal-sluiting

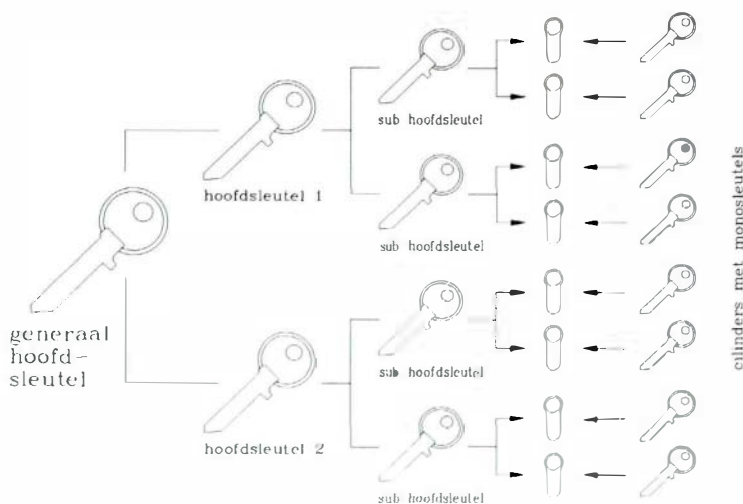




Systeem C
Centraal-sluiting met
hoofdsleutel



Systeem D
Hoofdsleutelsysteem



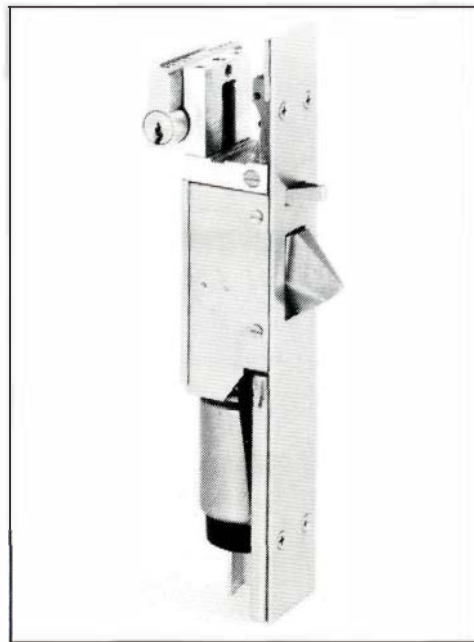
Systeem E
Generaal hoofdsleutel-
systeem

links:

Elektrische deurgrendel

rechts:

Elektrische deuopeners

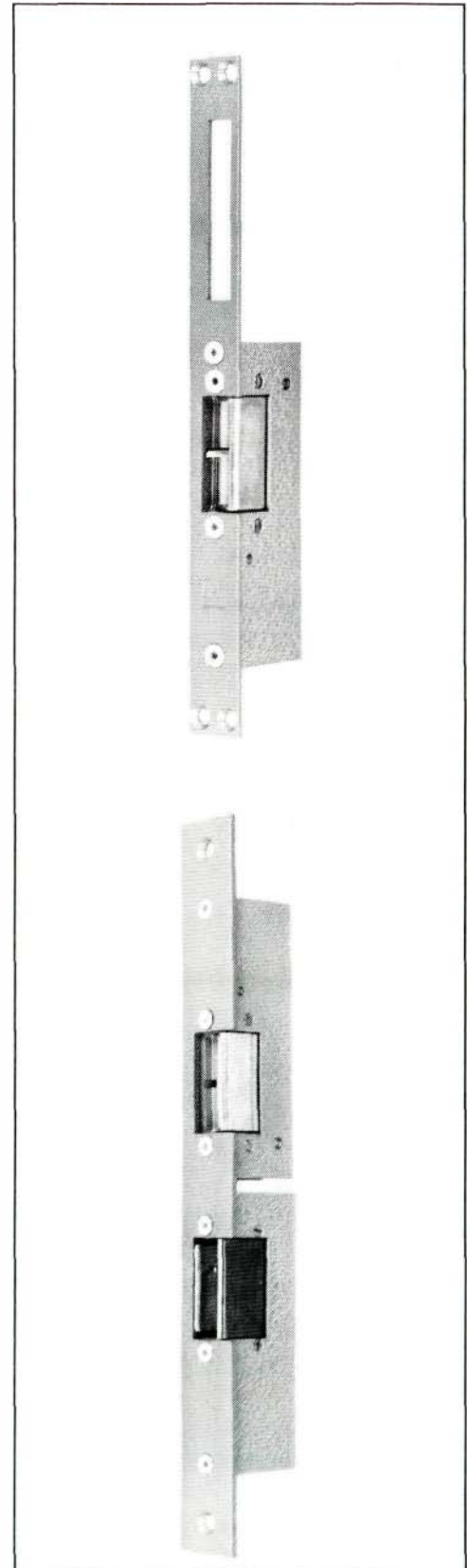


(vervolg van pag. 107)

Er zijn ook uitvoeringen die naar keuze de dag- of de nachtschoot vrijgeeft of beide. Om brandpreventieve redenen is de nachtschootdeuropener meestal uitgevoerd in het ruststroom-principe (spanningsloos = ontgrendeld). Er zijn tal van speciale uitvoeringen voor de gebruikelijke deurtypen, maar ook voor vluchtdeuren, volglasdeuren enz.

De speciale beveiligingsuitvoeringen kunnen een weerstand op het kantelbare deel opbrengen die overeenkomt met de eisen van NEN 5089. Dit type dient in die situaties te worden toegepast als er naast toegangscontrole ook eisen voor inbraakbeveiliging zijn. Er dient dan steeds een type te worden toegepast dat werkt op de *nachtschoot* en voorzien is van micro-switches en contacten voor de signalering.

Een veel voorkomende fout bij toepassing van elektrische deuopeners is het gebruik van een te licht of ondeugdelijk type deuopener, reden waarom men nogal eens slecht functionerende, gemakkelijk te saboteren of niet-functionerende (toegangsbeveiligings)situaties aantreft. Ook de montage verdient veel zorg, en dient bij voorkeur te geschieden door ervaren specialisten op dit gebied.



Elektromotorsloten

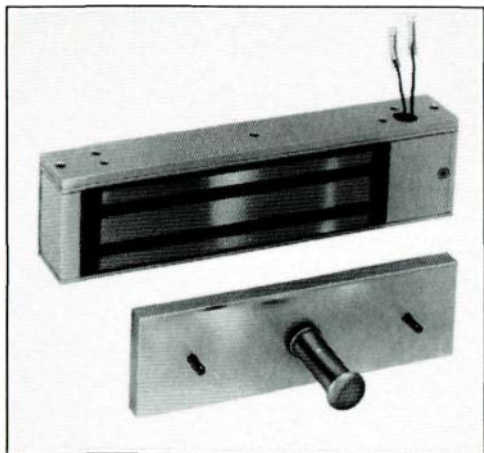
Bij een elektromotorslot wordt de nachtschoot van het (insteek)slot voortbewogen door een kleine maar zeer krachtige elektromotor. Hiermee kan men de deur ver- of ontgrendelen. Ook kan men ter plaatse van de deur het slot met een cilinder met de sleutel bedienen. In het slot zijn doorgaans micro-switches ondergebracht die de (uiterste) schootstanden naar het bedieningstableau kunnen doorgeven. De sloten zijn verkrijgbaar in een inbraakwerende kwaliteit die op het niveau van de NEN 5089 ligt, of hoger.

Elektromagnetische deurvergrendelingen

Een elektromagnetische deurgrendel bestaat uit twee delen: een elektromagneet en een ankerplaat. Doel van dit type grendel is om deuren op afstand te openen of te vergrendelen.

De elektromagneet wordt in principe aan de bovendorpel van het kozijn gemonteerd, en de ankerplaat met behulp van speciale bevestigingsmiddelen aan het deurblad.

De deur wordt met krachten van 700 kg of meer vergrendeld, terwijl bij onderbreking van de spanning, bijvoorbeeld bij een calamiteit, er volledige zekerheid is van een ontgrendelde deur. Op de grendel zijn doorgaans micro-switches aangebracht voor de deurstatus en als beveiliging tegen sabotage van de behuizing. Er



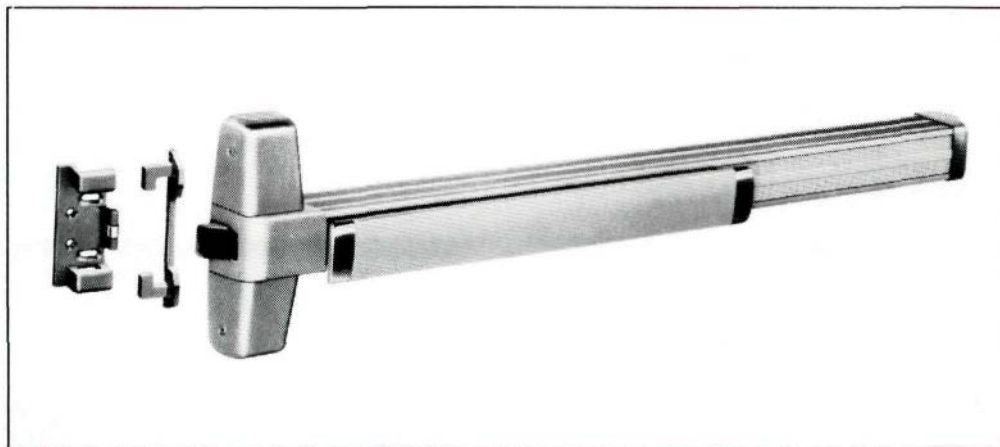
Elektromotorslot

zijn ook kleinere uitvoeringen met een geringere houdkracht (< 300 kg). Hier van kunnen er bijvoorbeeld twee stuks aan onder- en bovenzijde in de kozijnstijl aan sluitzijde ingelaten worden gemonteerd. De elektromagnetische deurvergrendelingen zijn bijzonder geschikt voor nooduitgangsdeuren, maar kunnen soms ook voor veel-gebruikte toegangsdeuren worden toegepast. De elektromagneten dienen bij toegangsdeuren een te verwaarlozen remanent magnetisme te hebben daar dit anders als hinderlijk wordt ervaren. Een remanent magnetisme mag maximaal circa 0,25 sec. voelbaar aanwezig zijn. Een elektromagnetische grendel kent geen bewegende delen, en dus een te verwaarlozen vorm van slijtage. Er kan om die reden een hoger functioneel gebruik gewaarborgd worden dan met sommige elektrische deuropeners of grendels.

*links:
Elektromagnetische
deurvergrendeling*

Deursluiters — deuropeners

De meest hoogwaardige apparatuur op het gebied van deurbeveiliging heeft weinig zin, wanneer de deur na gebruik niet automatisch wordt gesloten. Bij een elektrischbediende schuifdeur is dit geen probleem, maar bij een draaideur zal een voldoende sterke deurdranger moeten

Paniekopener

worden toegepast. De doorgaans zwaar belaste dranger dient op zeer deugdelijke wijze (bij voorkeur door een specialist) te worden gemonteerd.

De traditionele deurdranger wordt steeds meer vervangen door volautomatische draaideuraandrijvingen die boven de deur op het kozijn worden aangebracht. Net als bij een dranger wordt de deur met een 'sterke arm' dichtgetrokken. Na aansturing door een sensor, drukknop of toegangscontrolesysteem opent deze volautomatische deurdranger (of draaideuraandrijving) de deur. Openings- en sluitsnelheden, openings- en sluitdemping, openingshoek enz. zijn bij dit soort aandrijvingen (elektro-hydraulisch of elektro-mechanisch) zeer nauwkeurig regelbaar. De deuropeningshoek is doorgaans maximaal 100 graden, de sluittijd 3–6 seconden, en de openingstijd 2–5 seconden.

Paniekopeners

Paniekopeners of anti-panieksluitingen worden bij deuren in vluchtwegen toegepast. Bij een calamiteit moeten deze deuren door middel van hun speciale vergrendeling de garantie geven dat ze onder alle omstandigheden (waaronder 'paniek') snel, en op zeer eenvoudige wijze in vluchtrichting kunnen worden geopend. Zeer tegengestelde belangen treffen we aan als naast genoemde vluchteisen ook nog eisen op het gebied van inbraakwerendheid en/of toegangscontrole van toepassing zijn.

In hoofdstuk 7 onder: Daken en vluchtwegen kwam dit onderwerp reeds ter sprake. De hang- en sluitwerkindustrie heeft zich dit onderwerp goed aangetrokken, en in de praktijk kan tegenwoordig vrijwel volledig worden voldaan aan de eisen van enerzijds het vluchten, en anderzijds de inbraakbeveiliging en de controle op het gebruik van dit soort deuren. Het vaak 'roestige', slecht functionerende stangstelsel, dikwijls voorzien van niet-geoorloofde kettingen met hangsloten en dergelijke, behoort hiermee tot het verleden. Bij toepassing van een voldoende stijf (inbraakwerend) deurblad (hout, staal of aluminium), al dan niet voorzien van slagwerend glas, kan op één punt in voldoende mate inbraakwerend worden afgesloten, dat wil zeggen met één voldoende lange en sterke schoot in een even sterke sluitkast of kom. Naast de nachtschoot wordt vaak ook nog een dagschoot toegepast. Voor het bedienen van deze schoten wordt in vluchtrichting soms een duwplaat toegepast, maar meestal een horizontale duwstang op slothoogte. Op duwplaat of stang staat vaak om preventieve redenen aangegeven dat bij gebruik een 'alarm' volgt. Dat kan een in de slotbehuizing aangebracht akoestisch alarm zijn en/of een doorschakeling naar het inbraakalarm- en/of toegangscontrolesysteem.

De uitvoeringen van de paniekopeners zijn er qua gebruik veelal in twee soorten; alleen te gebruiken als uitgang, of als uit- en toegang, waarbij zich dan aan de bui-

tenzijde van de deur een slotcilinder bevindt.

De in elektronische zin meer uitgebreide versies kunnen op afstand alle gewenste informatie over de deurstatus (open/dicht), (nacht)schoot uit of in, pogingen tot sabotage enz. geven.

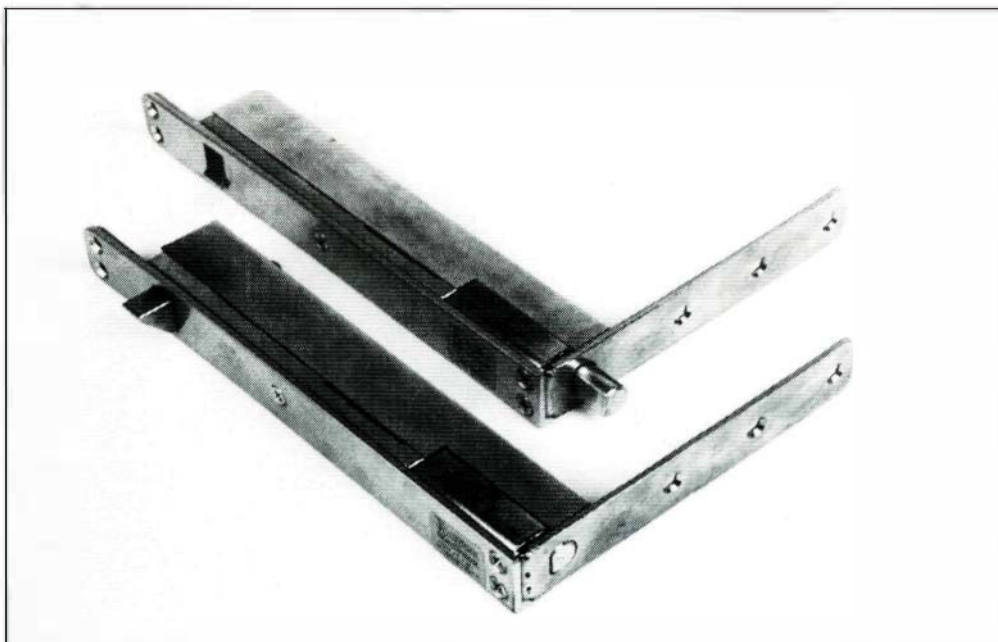
Automatische kantschuif en deurselector

De automatische kantschuif wordt toegepast voor het automatisch vergrendelen of ontgrendelen (aan boven- en onderzijde) van de helft van een dubbele deur. De deuren dienen in principe uitgerust te zijn met een deurselector, die ervoor zorgt dat één helft van de deur eerder sluit dan de andere. Op de eerste sluitende helft van de deur wordt aan boven- en onderzijde een kantschuif gemonteerd. Door het sluiten van de andere helft van de deur wordt een pal op de kantschuif ingedrukt, die ervoor zorgt dat de grendelpennen worden uitgeschoven en de deur wordt vergrendeld. Bij het openen van de deur wordt automatisch de andere helft weer ontgrendeld zodat dit geheel in combinatie met bijvoorbeeld elektrische deuropeners (in ruststroomuitvoering/spanningsloos = ontgrendeld) een uitstekende be-

veiliging biedt in panieksituaties, wanneer de uitgangen ontgrendeld dienen te zijn terwijl ze in normale omstandigheden zijn vergrendeld. Er zijn ook uitvoeringen verkrijgbaar waarbij het sluiten automatisch wordt vergrendeld, maar waarbij ontgrendeling met de hand dient te geschieden.

De deurselector wordt toegepast bij het selectief sluiten van dubbele deuren die zijn voorzien van een deurdranger, zoals hiervoor genoemd, meestal in combinatie met een automatische kantschuif en/of andere mechanische en/of elektrische vergrendelingen, waarbij het noodzakelijk is dat één helft van de dubbele deur eerder sluit dan de andere. De deurselector wordt aan de aanslagzijde van het deurkozijn op de bovendorpel gemonteerd.

De werking van de deurselector berust op de samenwerking van twee geleideballen. De ene deurelhelft wordt zo lang opgehouden totdat de andere deurelhelft bij het sluiten de geleidepal heeft ingedrukt, waarna de andere deurvleugel kan sluiten. Er is een beveiliging aangebracht die bij (opzettelijk) foutief en/of geforceerd gebruik schade aan deur, scharnieren en selector voorkomt.



Automatische kantschuif

Bedieningspanelen

Voor de op afstand bediende beveiligde deuren bestaan verschillende bedienings- of stuureenheden. Bij (grotere) toegangscontrolesystemen kan de aansturing bijvoorbeeld via het gebruik van een kaartlezer bij de deur geschieden. Bij één deur of bij een gering aantal beveiligde deuren kan op afstand een drukknop worden gebruikt. De deur ligt dan in het zicht van de 'bewaking', of er wordt via intercom en/of gesloten televisiecircuit onderhandeld over de toegang. Andere mogelijkheden zijn het gebruik van een sleutelschakelaar, of een paneeltje met toetstableau. Op het toetstableau dient bijvoorbeeld een viercijferige code te worden ingetoetst, waarna (bij juiste code) de deur voor een instelbare periode (0–30 seconden) wordt ontgrendeld. De code is op een zeer eenvoudiger manier te wijzigen. Een euvel is dat de code praktisch altijd door een ander kan worden meegelezen, zodat men op z'n minst de code frequent moet wijzigen.

Een betere oplossing is het gebruik van een toetsenpaneel met een 'scramble'-codesysteem. Door toepassing van een speciaal prisma in de doorzichtige toetsen worden de cijfers na het intoetsen van de 'start'-toets zichtbaar binnen een hoek van circa vier graden voor het tableau. Dat wil zeggen dat de cijfers alleen zichtbaar zijn voor de gebruiker die recht voor het tableau staat. Na het intoetsen van de juiste code verdwijnen de cijfers. Na het weer intoetsen van de 'start'-toets verschijnen de cijfers weer, maar nu in een geheel andere volgorde ('scramble'). Probeert men dus door het bedienen van de 'afgekeken' toetsen toegang te verkrijgen dan zal dat tevergeefs zijn. Op één of meerdere van dit soort pogingen kan eventueel een alarm in werking treden.

DEURENBOEK

Het aantal beveiligde deuren in een wat groter beveiligingsplan is soms niet gering. De details per deur verschillen nogal

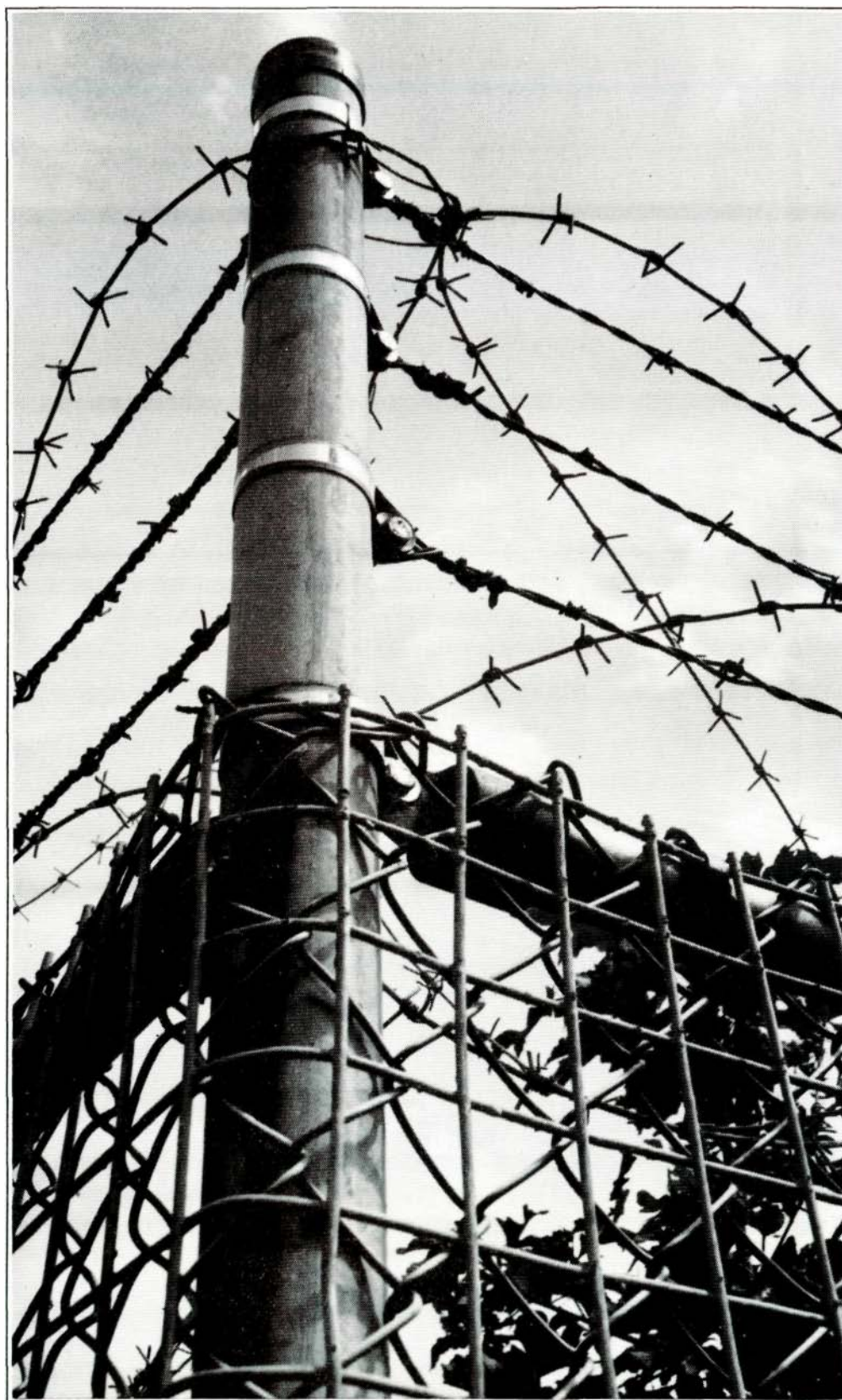
eens, en het mag derhalve duidelijk zijn dat een en ander goed moet worden begeleid om misverstanden te voorkomen, elkaar tijdens de montage niet voor de voeten te lopen, en niet twee of meerdere keren (nagenoeg) hetzelfde werk te doen. Een goed hulpmiddel hierbij is een 'deurenboek'. Al in het ontwerpstadium wordt consequent elke deur in het boek genoemd, met een schets van de situatie waarop alle details staan aangegeven. Zo zal voor een beveiligde draaideur bijvoorbeeld in detail aandacht moeten worden gegeven aan meerdere punten van onderstaand rijtje:

- deurbladmateriaal/afwerking;
- draairichting, openingshoek, aanslag;
- deurdranger;
- hoofdsloot;
- scharnieren;
- beslag;
- glasopening(en);
- glasopsluiting;
- deurspion;
- elektrische deurgrendels;
- elektrische deuropener;
- elektromotorsloot;
- elektromagnetische deurvergrendeling;
- (elektrische) deursluitersopener;
- paniekopeners;
- automatische kantschuif en deurselector;
- bedienings- of toetsenpaneel;
- intercom;
- kaartlezer;
- reedcontacten voor deurstandsignalering;
- micro-switches voor schootstandsignalering;
- bevestiging voor televisiecamera;
- enz.

De schets geeft aan hoe een blad uit een dergelijk deurenboek eruit kan zien.

Voorbeeldblad van een
deurenboek

BEVEILIGING	GEBOUW: E	DEUR: 0.12
SPECIFIKATIE		
1 = plafond-verlichtingsarmatuur (CCTV)		
2 = magneetcontact, inbouw		
3 = kaartlezer, inbouw		
4 = elektrische deuropener, inbouw		
5 = kabelgoot		
6 = aansluitpunt CCTV-camera		
7 = systeemplafond		
8 = deurdranger		
9 = slagwerend glas met glasbreukdetectie		
10 = glaslatten		
11 = kabeldoorvoer, inbouw (niet zichtbaar)		
12 = insteek-cilinderslot met beslag		
13 = deurbladmateriaal		
14 = scharnieren		

Technische afscheiding

Met de toenemende trend om kantoren buiten, of aan de randen van, de bebouwde kom te situeren, beschikt men doorgaans over een aan het gebouw grenzend terrein. Dit dient voor de aan- en afvoer, als parkeerplaats, maar kan ook dienst doen bij de algehele beveiliging van het bedrijf. Allereerst moet worden vastgesteld met welk doel een terreinbeveiliging wordt aangelegd. Terwijl het onder normale omstandigheden de voornaamste reden van een afbakening is, om aan te geven dat men een bepaald terrein nadert en dreigt te betreden, gaan we er hier vanuit dat het de bedoeling is om daarnaast het volgende te bereiken, dat de beveiliging als afschrikmiddel dient, binnendringen vertraagt en signaleert. Het uitgangspunt daarbij is dat mensen worden tegengehouden; daarnaast kunnen voertuigen geleid worden. Bij de uitvoering van de afscheidingen en bij het aanbrengen ervan, moet rekening worden gehouden met de drie manieren waarop deze hindernissen genomen kunnen worden: *door*, *over* of *onder* de hindernis.

Ten eerste kan men, al of niet met geweld, *door* de hindernis heen het doel proberen te bereiken. Hiervoor is het dus zaak om de hindernis zodanig uit te voeren, dat het verbreken van de afsluiting zo moeilijk mogelijk is en dat er zo min mogelijk zwakke plekken zijn.

Ten tweede kan men proberen, met of zonder hulpmiddelen, *over* de hindernis te klimmen. Hiervoor dient de uitvoering zo te zijn, dat het materiaal zo min mogelijk steun voor klimmen biedt en ook zo hoog (en eventueel 'slap') is, dat overklimmen moeilijk is. De aanwezigheid van opstapjes in de buurt van een hek, bijvoorbeeld bomen of bouwsels, moet worden voorkomen.

Ten derde kan men juist *onder* de afscheiding door willen komen. Dit vereist doorgaans meer werk, maar kan minder zichtbaar gebeuren. De detaillering van een afscheiding moet hierop worden aangepast.

AFSCHEIDINGEN

Er zijn verschillende soorten afscheidingen toe te passen, waarbij we hier een tweedeling maken in afscheidingen die zijn gemaakt van voornamelijk natuurlijke materialen, die mooi in een omgeving

kunnen worden ingepast, en technische afscheidingen.

Natuurlijke afscheidingen

Uit het oogpunt van mensvriendelijkheid en esthetiek, kan het de voorkeur verdienen om afscheidingen te maken, die er plezierig uitzien. Te denken valt daarbij aan de volgende afscheidingen.

Wallen

Voor het tegenhouden van voertuigen kunnen wallen een goede functie hebben. Voor het tegenhouden van personen wordt slechts in combinatie met andere maatregelen iets bereikt. Daarbij moet worden gedacht aan observatiemogelijkheden, waarvoor verlichting, manbewaking en eventueel televisiecamera's noodzakelijke aanvullingen zijn.

Sloten en grachten

Sloten en grachten zijn eveneens effectief voor het tegenhouden van voertuigen; voor het tegenhouden van personen zijn zij dit alleen als zij breed genoeg zijn. Bovendien moeten de oevers zodanig steil zijn, dat het moeilijk is om ze vanuit het water te beklimmen en moet de diepte van

Natuurlijke afscheiding (water)



het water zodanig zijn, dat men niet naar de overkant kan waden. Om het gebruik van vaartuigen te voorkomen, is het gunstig om een open verbinding met vaarwegen te vermijden, waardoor de aanwezigheid van boten altijd zal opvallen. Ook hier geldt, net als bij wallen, dat aanvullend moet worden gewerkt met het actief of passief observeren van de natuurlijke barrière. Een vaak vergeten probleem bij sloten en grachten wordt gevormd door een simpel klimatologisch gegeven: water kan in de winter bevriezen.

Hagen en struiken

Als aanvulling op andere maatregelen is het aanbrengen van moeilijk doordringbare hagen en struiken een mogelijkheid. Wel moet opgepast worden, dat niet juist een verkeerde hulp wordt geboden, doordat visuele bescherming wordt gemaakt of de mogelijkheid tot opstappen. Heesters met doornen kunnen uiterst lastig zijn en ook geven heesters de mogelijkheid om andere hindernissen te verstoppen.

Technische afscheidingen

Doorgaans effectiever en beter naar wens te moduleren dan natuurlijke afscheidingen,

zijn afscheidingen van — over het algemeen — niet-natuurlijke materialen, die per meter zijn te plaatsen door de aannemer of een hekwerkspecialist.

Muren

Muren kunnen van baksteen worden gemetseld of worden samengesteld uit grotere elementen, bijvoorbeeld van beton. Bij een gesloten uitvoering bestaat een volledige afsluiting van de buitenwereld, die echter vaak kostbaar is en moeilijk in overeenstemming te brengen met eisen, die bijvoorbeeld een welstandscommissie in een stedelijke situatie stelt. De hoogte van de muren moet voldoende zijn, er mogen geen steunen voor klauteraars zijn en de bovenkant mag geen makkelijk bevestigings- of steunpunt zijn.

Schuttingen

Deze zijn in principe te vergelijken met muren, maar doorgaans uitgevoerd in minder duurzame materialen en worden derhalve toegepast in situaties die minder hoge eisen stellen aan de beveiliging. De kwaliteit wordt voornamelijk bepaald door het gebruikte materiaal en verder door de uitvoering van dezelfde details,

waarvoor bij de muren aandacht werd gevraagd.

Hekwerken

Bij hekwerken bestaat, zowel van binnen naar buiten als andersom, een goed zicht. Dit heeft voordelen maar ook nadelen, ten opzichte van ondoorzichtige afscheidingen. Er zijn aan hekwerken een aantal eisen te stellen die ook voor muren gelden:

- voldoende hoogte;
- voldoende beveiliging van de bovenkant van het hek voor overklimmen en de onderkant voor ondergraven;
- zo min mogelijk aansluitingen op bijvoorbeeld gebouwen;
- de afwezigheid van allerlei opstapjes.

Daarnaast moet aandacht worden besteed aan de maximale afstand van de palen, moet de bevestiging van het metaalgaas, stekmetaal of (prikkel)draad aan de palen van voldoende sterkte zijn en moet dat materiaal zelf niet makkelijk door te knippen zijn, hetgeen echter altijd mogelijk zal blijven. Beter bestand tegen doorknippen zijn hekwerken die zijn opgebouwd uit stalen spijlen, bevestigd aan liggers en staanders. Deze geven helaas meer houvast voor overklimmen en zijn veel duurder dan gewone gaashekwerken.

Niet ongenoemd mogen de hekwerken blijven, waar het basismateriaal bestaat uit slagvast glas, bevestigd tussen palen. Dit is een dure uitvoering van een hekwerk, misschien meer te vergelijken met een schutting, die daar kan worden toegepast waar buitengewone eisen worden gesteld aan zowel de esthetische als de technische uitvoering.

POORTEN EN OBSTAKELS

Op welke wijze een afscheiding ook is uitgevoerd, de zwakke plek daarin wordt gevormd door de openingen die moeten worden gemaakt om naar binnen en buiten te kunnen gaan. Daarom mogen niet meer toegangen worden gemaakt dan strikt noodzakelijk is. Daarbij moet onderscheid worden gemaakt tussen toegangen voor personen en voor voertuigen. De toegang moet zodanig worden uitgevoerd, dat de poort buiten werktijd goed kan worden afgesloten en een waardig onderdeel van de afscheiding vormt. Onder werktijd moet de poort te controleren zijn, zonodig door middel van een directe controle van alle passanten. Dit kan gebeuren vanuit een portiersloge of iets dergelijks aan de rand van het terrein of vanuit een gebouw met zicht op de



Poort

terreintoegang, aangevuld met toegangscontrolesystemen en/of gesloten televisiesystemen. Deze bewakingsposten kunnen ook een rol spelen in de permanente bewaking en het beheer van de gebouwen. Voor de doorgang van personen kan worden gedacht aan draaipoorten, aan tourniquets of aan sluizen. Als tevens met een toegangscontrolesysteem wordt gewerkt, zal een van de twee laatste oplossingen moeten worden gekozen.

Voor de doorgang van voertuigen kan gekozen worden uit draai- of schuifpoorten. Bij frequent gebruik van de poort kan gekozen worden voor toevoeging van een slagboom, die makkelijker te bedienen is. Bij signalering van onraad kan alsnog de poort worden gesloten, om in- of uitrijden te vermijden.

Indien gevreesd wordt dat de poort of het hekwerk met een voertuig zal worden geraamd, kunnen obstakels in de vorm van grote blokken of bloembakken de rijnsnelheid nabij een poort zodanig verlagen, dat het gevaar daarvoor afneemt. Dit is weer goed te combineren met een slagboom, die meer een visuele en signalerende werking heeft dan dat voertuigen kunnen worden gestopt.

CONTROLE

Het is bij alle afscheidingen van belang dat controle wordt uitgeoefend op de afscheiding en de omgeving. Het gaat daarbij om een aantal facetten. De afscheiding moet frequent worden gecontroleerd op haar effectiviteit. Beschadigingen of doorboringen moeten snel worden gesignaleerd en gerepareerd en het onderhoud vraagt voortdurende aandacht. Ook de directe omgeving van de afscheiding vraagt steeds om controle op de aanwezigheid van opstapjes enz. Daarnaast moet steeds worden gecontroleerd of pogingen worden (of zijn) gedaan om de hindernis te nemen.

Als geconstateerd wordt dat geprobeerd is of wordt om de afscheiding te nemen, zal onmiddellijk actie moeten worden genomen om de schade te kunnen beperken.

Het hangt van de organisatie van de beveiliging af, of hiervoor politie en/of bewakingsdienst wordt ingeschakeld of dat men zelf de eerste stappen neemt.

Het constateren van een poging tot binnendringen kan worden gesignaleerd door een in of aan de afscheiding ingebouwd systeem of door een signalering meteen voor en/of achter de afscheiding, bijvoorbeeld op basis van bewegingsdetectie. Bovendien kan eventueel met een gesloten televisiesysteem permanent worden gevolgd of er zich mensen in de buurt van de afscheiding ophouden of pogingen doen erdoor of overheen te komen. Of het gebruik van dit soort apparatuur zinvol is hangt ook weer volledig af van de organisatie van de beveiliging door de gebruiker van het kantoorgebouw.

PARKEERPLAATSEN

Onder werktijd zal een parkeerplaats van een kantoor gebruikt worden door werknemers en bezoekers. Er wordt op dat moment wel of geen controle uitgeoefend, maar wel bestaat er een soort sociale controle tegen diefstal of vandalisme door de aanwezigheid van mensen. Buiten werktijd zal de parkeerplaats leeg zijn. Het is goed om deze buitenruimte op dat moment binnen de beveiliging van het terrein een rol te laten spelen door te zorgen dat vanwege de lege parkeerplaats een goed zicht bestaat op de gebouwen. Dit kan zijn vanaf de openbare weg, zodat surveillanten snel en goed zicht hebben, of vanuit een speciale bewakingsruimte. Het is natuurlijk wel zaak om de parkeerplaats niet vol struiken of andere obstakels te zetten, waardoor het zicht alsnog slechter wordt.

VERLICHTING

Op het gehele buitenterrein moet een buitenverlichting worden aangebracht, die het mogelijk maakt om bij surveilleren het hele gebied goed te overzien. Er zullen daarvoor op beperkte afstanden van elkaar armaturen aangebracht moeten wor-

den, op lantaarnpalen of aan de muren van gebouwen. De lampen moeten alle hoeken en gaten die niet kunnen worden vermeden, aanlichten en daarnaast een ring om het gebouw vormen. Indien een beveiliging met een hek zodanig is gemaakt, dat daarop overdag goed zicht mogelijk is, kan deze nog worden versterkt door het aanbrengen van lampen direct op of na de afscheiding, waardoor overklimmen ook in het donker goed opvalt. De lampen moeten op zodanige hoogte worden aangebracht, dat ze niet makkelijk zijn te bereiken. Het is desalniettemin aan te raden om als armatuur te kiezen voor een slagvaste uitvoering, zodat ook voor steengooiende vandalen enige weerstand bestaat. Voor de bediening kan worden gekozen tussen een normaal, eventueel tijdgeschakeld systeem of een systeem dat, centraal of decentraal, wordt geschakeld door lichtgevoelige cellen. Hierdoor ontstaat een groter bedieningsgemak. In elk geval moet de verlichting zodanig worden uitgevoerd dat in geval van een beperkte storing, zoals een uitgevallen lamp of een kapotte lichtcel, niet grote delen van het terrein in het donker liggen. Een andere mogelijkheid is het aanbrengen van zogenaamde schrikverlichting, die in werking treedt zodra iemand daarbij in de buurt komt. Deze mogelijkheid is doorgaans zeer effectief, tot het moment dat de onverlaten daarvan op de hoogte zijn en vervolgens gewoon verder hun gang gaan. Zeker op afgelegen terreinen zal niemand acht slaan op het licht dat blijft branden. Combinatie met alarmering kan hier echter uitkomst bieden.

GESLOTEN TELEVISIESYSTEMEN

Aanvullend op afscheidingen van terreinen, kan het noodzakelijk zijn om gebieden in de gaten te houden, zowel tijdens werktijd als in de avonduren. Bovendien kan het ook wenselijk zijn om de bedrijfsactiviteiten overdag steeds te volgen, waardoor een combinatie mogelijk is. In dat geval kan overwogen worden om een gesloten televisiecircuit aan te brengen.

We zullen hier geen volledige uitleg van een dergelijk systeem geven of verschillende systemen met elkaar vergelijken, maar enkele aandachtspunten kunnen nuttig zijn.

Overzicht:

Allereerst moeten voor de terreinbeveiliging de camera's zo worden opgesteld, dat het hele terrein te overzien is of dat bijvoorbeeld de hele afscheiding met de openbare weg kan worden gezien. Dit kan door middel van vaste en/of draaiende camera's, waarbij een voorkeur uitgaat naar vaste, omdat bijvoorbeeld bij vermeend onraad met een draaibare camera niet snel teruggedraaid kan worden naar de gewenste plek.

Plaatsing camera's:

De camera's kunnen zowel binnen als buiten het gebouw worden geplaatst. In het eerste geval moet gezorgd worden dat reflecties worden tegengegaan, in het tweede geval moet gezorgd worden voor een weerbestendige behuizing van de camera's.

Kwetsbaarheid:

De buitencamera's moeten natuurlijk op zodanige hoogte worden aangebracht, dat ze buiten bereik van vandalen, inbrekers enz. zijn.

Ook moet gezorgd worden dat ze redelijk bestand zijn tegen het gooien met stenen en dergelijke.

Verlichting:

Bij gebruik van televisiebewaking moet voor het bewaakte terrein gezorgd worden voor een verlichting, die is afgestemd op de mogelijkheden van de camera. Dat houdt in dat de gewenste kleur van het kunstlicht, de benodigde hoeveelheid licht, maar vooral ook de kijkhoek van de camera's ten opzichte van de lichtbronnen nauwkeurig moeten worden bepaald.

Onderhoud:

Bij gebruik van een televisiesysteem moet regelmatig controle en onderhoud plaatsvinden van de camera's, de camera-behui-

zing, de bekabeling en de monitors, omdat storingen vermeden moeten worden.

Controle:

Voor het volgen van de beelden, voor het signaleren van onraad en voor het nemen van maatregelen, moet ergens een ruimte bestaan. Dit kan op het bewaakte terrein zelf zijn, maar het kan ook in de nabije omgeving zijn, bijvoorbeeld bij een centrale bewakingsruimte die functioneert voor meerdere kantoren in de omgeving.

BEWAKINGSRUIMTEN

Aanvullend op verschillende van de genoemde maatregelen, moeten er mensen zijn, die hetzij een oogje in het zeil of op het scherm houden, die een toegangscontrolesysteem beheren of optreden als er op enigerlei wijze alarm wordt geslagen. Onder werktijd kan dit in een deel van het gebouw gebeuren, bijvoorbeeld nabij de ingang, maar er kan ook een portiersloge aan de rand van een terrein worden ingericht. De keuze moet worden gedaan aan de hand van de te verwachten activiteiten. Voor buiten werktijd zal vaak extra bewaking worden ingezet, soms in eigen dienst en soms door middel van een bewakingsdienst. Met name op bedrijfsverzamelterreinen wordt de controle in toenemende mate door bewakingsdiensten uitgeoefend, in opdracht van de gezamenlijke bedrijven. In een dergelijk geval, moet ook een eigen ruimte beschikbaar zijn. Deze zal bij voorkeur niet in een gebouw gelegen zijn, maar daarbuiten, liefst geheel onafhankelijk. Het moet worden vermeden, dat de bewakers toegang hebben tot het gebouw, het is voldoende als zij in geval van onraad contact opnemen met de politie of met het betreffende bedrijf.

Vanaf het eind van de jaren zeventig is de belangstelling voor het verschijnsel vandalisme sterk toegenomen. Deze aandacht wordt mede ingegeven door de omvang waarin het probleem zich aandient. In het tweede deel van de serie Beveiliging van gebouwen wordt uitgebreid ingegaan op de achtergronden van vandalisme en de bouwtechnische mogelijkheden voor vandalismepreventie. In dit hoofdstuk geven we daarom slechts een kort overzicht van enkele punten met betrekking tot dit delict. Voordat we daarbij naar de cijfers gaan kijken zullen we allereerst kort ingaan op het begrip vandalisme en de problemen die daarmee gemoeid zijn.

Wat is vandalisme?

Onder vandalisme verstaan wij vrij vertaald naar artikel 350 Wetboek van strafrecht: "het opzettelijk vernielen, beschadigen of onbruikbaar maken van bepaalde objecten". Uit de definitie blijkt dat lang niet alle vernielingen c.q. beschadigingen onder vandalisme vallen. Een automobilist die de macht over het stuur verliest en een paal een kopje kleiner maakt, kan moeilijk als een vandaal bestempeld worden. En daarmee begint het probleem ... Het zal immers lang niet altijd mogelijk zijn om in geval van een vernieling te achterhalen of er opzet in het spel was. Dit probleem van de meestal onbekende dader en de daardoor onbekende motieven heeft twee belangrijke gevolgen. Ten eerste geeft het waarschijnlijk aanleiding tot onevenredig veel onrustgevoelens onder burgers. Tekenend in dit opzicht is dat men vaak spreekt over "het zinloze vandalisme". Een tweede gevolg van het feit dat het *waarom* van de meeste vernielingen onduidelijk blijft, is dat daardoor niemand eigenlijk goed weet wat er zou moeten gebeuren ter bestrijding van het vandalisme.

Voordat men overgaat tot het treffen van maatregelen zal men in voorkomende gevallen dan ook eerst moeten zien te achterhalen of er opzet in het spel is, en zo ja, wie verantwoordelijk zijn voor de vernielingen en wat de redenen zijn waarom zij dat doen. Pas dan kunnen adequate maatregelen getroffen worden.

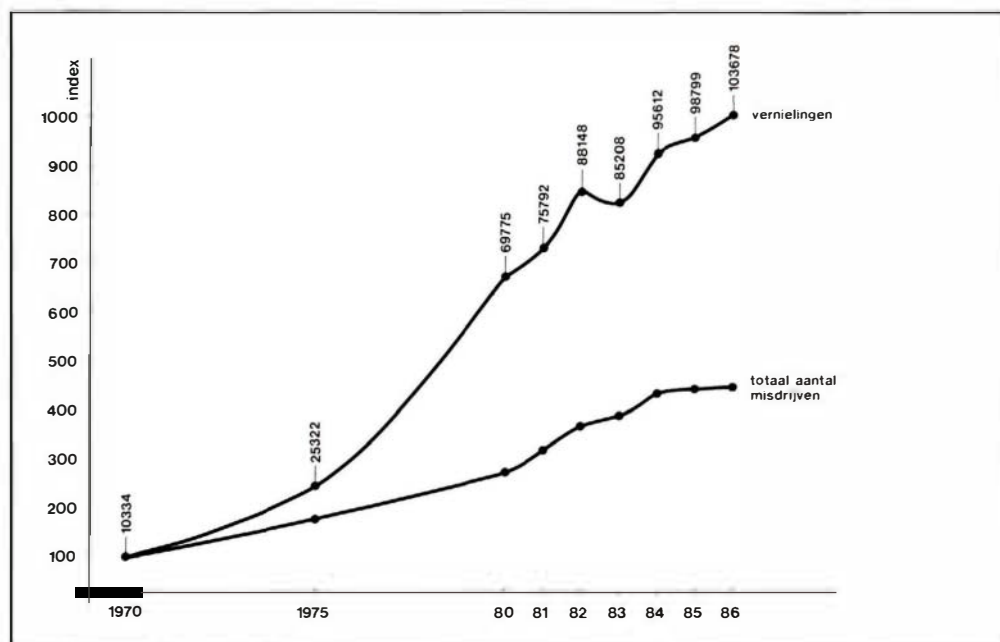
CIJFERS EN GEGEVENS OVER VANDALISME

Privé-bezit

Er bestaan twee belangrijke bronnen die een beeld geven van het aantal vernielingen dat in Nederland wordt gepleegd. Allereerst kunnen we kijken naar het aantal in de politie-statistieken geregistreerde vernielingen. De figuur (zie pag. 124) laat een duidelijke toename zien van het aantal door de politie geregistreerde vernielingen. Het aantal geregistreerde vernielingen eist ook relatief binnen het totale aantal misdrijven een steeds groter aandeel voor zich op. Bij deze figuur moet men echter wel bedenken dat het aantal vernielingen dat in werkelijkheid heeft plaatsgevonden behoorlijk zal verschillen van het aantal vernielingen dat in de figuur is terechtgekomen. Lang niet alle burgers en instellingen doen immers aangifte van vernielingen waarvan ze het slachtoffer zijn geworden. Deze niet ter kennis van de politie gekomen strafbare feiten duidt men ook wel aan met de term 'dark number'.

Om een beter idee te krijgen van de werkelijke hoeveelheid strafbare feiten die plaatsvinden, worden slachtoffer-enquêtes uitgevoerd, waarbij men aan een groot aantal Nederlanders boven de vijftien jaar vraagt of zij in een bepaald jaar het slachtoffer geworden zijn van bepaalde strafbare feiten. Als uit zo'n enquête bijvoorbeeld blijkt dat 5% van de geïnterviewden opgeeft dat zij het slachtoffer geworden

*Ter kennis van de politie
gekomen vernielingen*



zijn van een vernieling, dan kan men ervanuit gaan dat ook ongeveer 5% van de gehele Nederlandse bevolking boven de vijftien jaar het slachtoffer van een vernieling geworden is.

Op basis van deze figuren zijn de volgende conclusies te trekken:

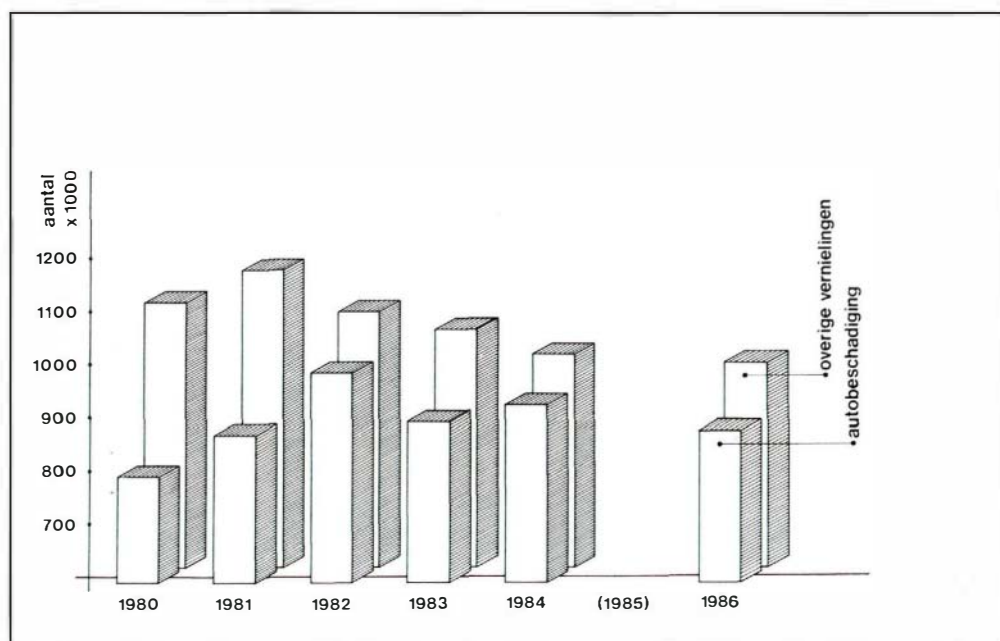
- Het aantal slachtoffers van vernielingen aan privé-eigendommen is tot het

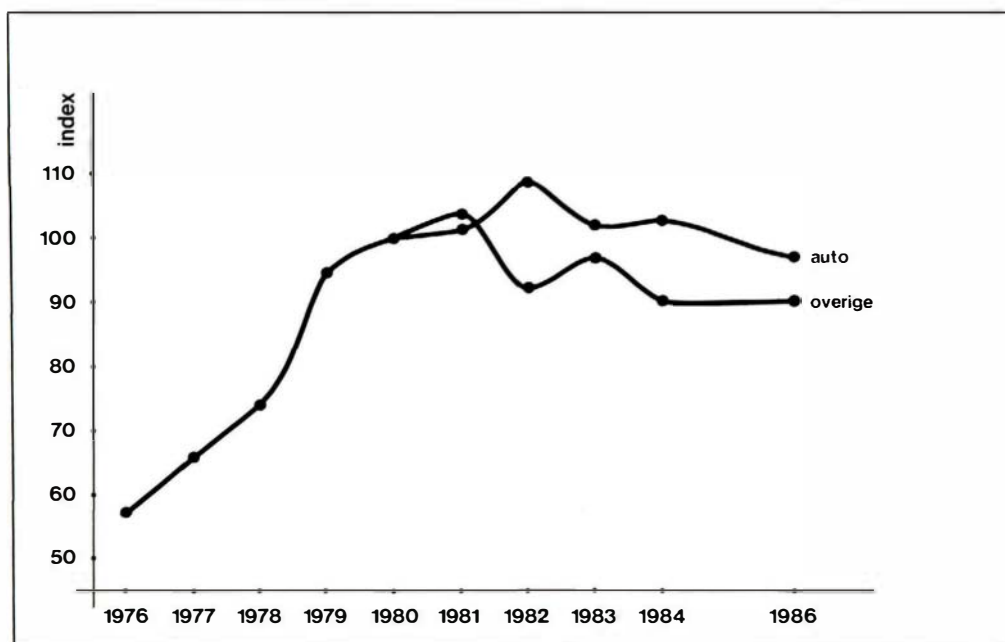
begin van de jaren tachtig sterk gestegen, daarna is een lichte daling te constateren.

De schatting (voor 1984) van de totale schade die met deze vernielingen aan privé-bezit gepaard gaat, komt ruim boven de 500 miljoen gulden uit.

Het blijkt dat er veel meer vernielingen plaatsvonden dan door de politie werden geregistreerd.

*Geschatte vernielingen
aan privé-bezit
(slachtoffer-enquêtes)*





Vernielingen aan privé-bezit: indexcijfers

Als we de politiecijfers vergelijken met de cijfers uit de slachtoffer-enquête blijkt dat het aantal vernielingen op basis van de slachtoffer-enquête minimaal (voor 1986) 16 keer en maximaal (voor 1981) 26 keer zo hoog was als het aantal aangiften dat door de politie werd geregistreerd. Daarbij moet bovendien nog bedacht worden dat vernielingen aan openbaar bezit buiten de slachtoffer-enquête blijven.

(Semi-)Openbaar bezit

Willen we een beeld krijgen van vandalisme aan (semi-)openbaar bezit dan zullen we een andere bron moeten aanboren. Op grond van onderzoek van de Vereniging van Nederlandse Gemeenten (VNG), dat gebaseerd was op speciaal opgezette vandalismeregistraties in 23 — qua grootte verschillende — gemeenten, is een voorzichtige uitspraak over de omvang van het vandalisme aan gemeentelijk bezit (dus slechts een deel van al het openbare bezit) mogelijk (VNG, 1984).

De volgende figuur (zie pag. 126) laat zien welke openbare objecten vooral de dupe worden van vandalisme. Scholen steken er met kop en schouders bovenuit, maar 'overige openbare gebouwen' mogen er ook zijn en hier kunnen we een relatie

leggen met kantoorgebouwen.

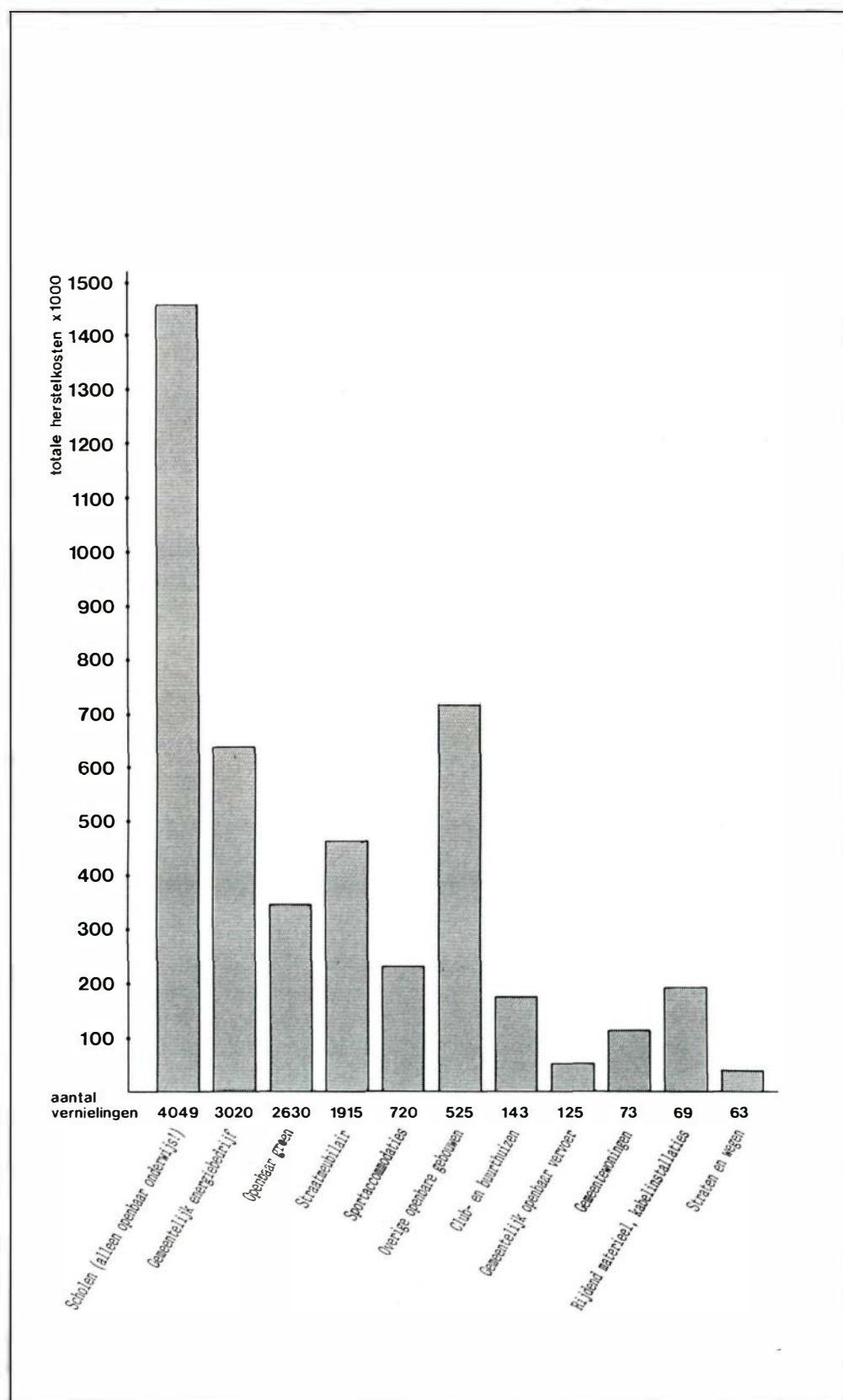
Op basis van de VNG-registratie kan een schatting worden gemaakt van de totale schade die vandalisme aan *gemeentelijk* bezit veroorzaakt. Deze schatting komt uit op 100 miljoen. Daarbij moet echter wel worden bedacht dat dit getal veel minder betrouwbaar is dan de schadebedragen die voor vernielingen aan privé-bezit zijn genoemd. Bovendien heeft deze schatting slechts betrekking op *gemeentelijk* bezit; er is nog veel meer openbaar bezit.

Bedrijfsbezit

Natuurlijk wordt ook bedrijfsbezit onderwerp van vandalisme: de winkel, het café, kantoorgebouwen, bedrijfsauto's, etc. Helaas is nauwelijks bekend hoeveel bedrijfsbezit jaarlijks vernield wordt. We beschikken slechts over twee incidentele bronnen:

- Op basis van een recent onderzoek van het EIM (Economisch Instituut Midden- en kleinbedrijf; zie ook hoofdstuk 2 en bijlage 4) is een schatting te maken van de schade die winkeliers ten gevolge van vandalisme lijden. Deze schatting komt uit op ruim 70 miljoen gulden, waarbij direct aangetekend moet worden dat filiaal- en grootwin-

*Vernielingen aan gemeen-
tebezit in 23 gemeenten
(VNG, 1984)*



kelbedrijven *niet* in het betreffende onderzoek waren betrokken (EIM, 1986).

- Een tweede onderzoek betreft een onderzoekje gehouden onder bouw-aannemers in Amsterdam en omgeving. Daaruit kwam naar voren dat op bouwplaatsen in de provincie Noord-Holland in 1984 al voor meer dan zeven miljoen gulden vernield werd. Alle geënquêteerde aannemers bleken slachtoffer van vandalisme te zijn (Van Dijk en De Savornin Lohman, 1985).

Een groot deel van de schade werd veroorzaakt door vernieling aan het bijna afgebouwde project zelf. Eigendommen van de aannemers (keten, loodsen, machines) moesten het echter ook ontgelden. Beide gegevens zijn zeer beperkt en onvolledig, als we praten over *het* bedrijfsleven. Een sector die in totaal 500.000 vestigingen omvat.

PREVENTIE BIJ KANTOORGEBOUWEN

Nu we enigszins een beeld hebben van de omvang van het probleem, concentreren we ons verder op mogelijk te nemen preventiemaatregelen.*

– Parkeerplaats:

De verlichting van het parkeerterrein moet ruim en overzichtelijk zijn.

– Muuropeningen:

Als openingen in buitenmuren noodzakelijk zijn, maak ze dan zo klein mogelijk en zorg dat ze bestand zijn tegen vandalisme en inbraak. Soms kan een dicht paneel in een kozijn een goede oplossing zijn.

– Bereikbaarheid:

Politie- en brandweervoertuigen moeten alle plaatsen goed kunnen bereiken.

– Glas:

Zorg voor slag- en kraswerend glas.

– Regenpijpen:

Over de onderste twee meter nooit regenpijpen toepassen die gemakkelijk beschadigd kunnen worden.

– Anti-graffiti:

Er zijn middelen in de handel om graffiti tegen te gaan dan wel weg te werken. Zie hiervoor ook SBR-publikatie nr. 170 en SBR-publikatie nr. 104 hoofdstuk 5.

– Ventilatie-openingen:

Een open stootvoeg is nog altijd het eenvoudigste middel om een gebouw te laten ventileren.

Overige ventilatievoorzieningen in de gevel, zoals bijvoorbeeld roosters, zijn gemakkelijk te beschadigen.

– Bestrating:

Vermijd de mogelijkheid om stenen en



*Afvalemmer ...
van ondeugelijke
kwaliteit?*

* = Hoofdstuk 7 van dit deel en hoofdstuk 5 van deel 3 geven daarbij de nodige bouwtechnische details aan.

tegels los te wrikken; de *ongelukken* kunnen juist in de kleine hockjes zitten.

– *Afvalemmers:*

Zorg dat wanneer er afvalemmers worden toegepast, deze van een goede kwaliteit zijn; ze moeten deugdelijk bevestigd zijn en (in verband met brandstichting) liefst niet tegen een gebouw of bij ramen. Ze moeten ook tegen een stootje kunnen.

– *Containers:*

Plaats afvalcontainers nooit onder een luifel. Een container staat het veiligst in een aparte, af te sluiten containerruimte. In de brochure *Schadepreventie bij afval en emballage van het TBBS* (voor het adres: zie bijlage 2) staat uitvoerig beschreven welke voorzorgsmaatregelen genomen kunnen worden om het brandgevaar zo klein mogelijk te maken.

– *(Brom)Fietzers:*

Terreinen rond kantoren dienen zoveel mogelijk vrij te zijn van (brom)fietzers; als er fietsen toegelaten worden, dan moeten er voldoende rijwielklemmen in de buurt zijn.

– *Fietsklemmen:*

Klemmen op (gemakkelijk los te maken) tegels zijn ongeschikt voor gebruik bij kantoren; ze moeten onwrikbaar verankerd zijn in de grond of aan een constructie.

– *Aantrekkingskracht:*

Pleinen hebben een grote aantrekkingskracht op jongeren; probeer die pleinen zoveel mogelijk vrij te houden van fietsers en bromfietsen.

– *Plantenbakken:*

Plantenbakken kunnen beter niet gevuld zijn met stenen, maar alleen met aarde. De constructie dient degelijk te zijn.

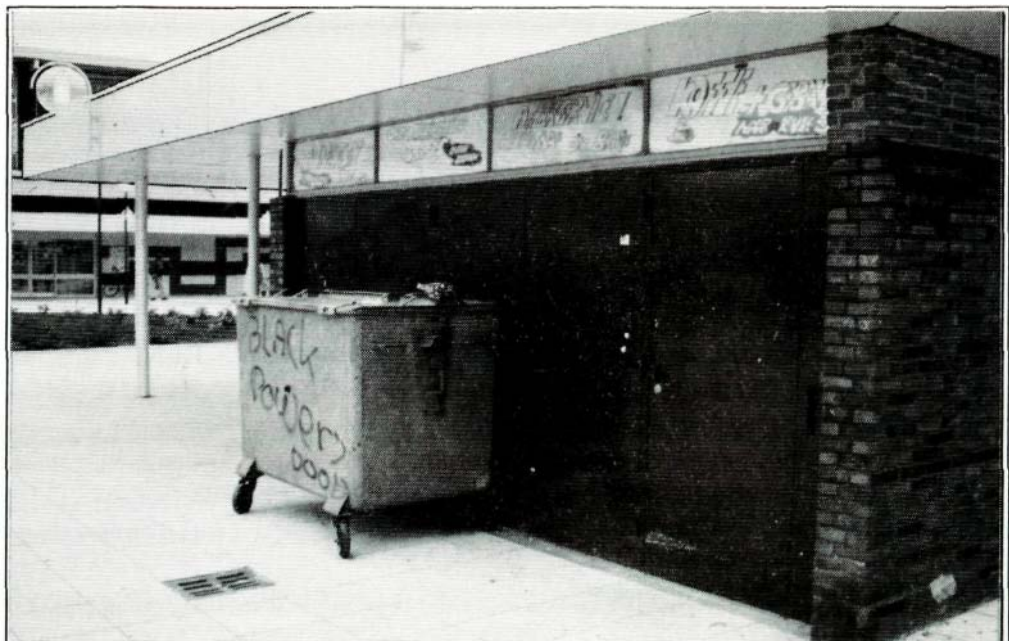
– *Buitenverlichting:*

Zorg voor slagvast materiaal voor de buitenverlichting en dergelijke. Let op losse bestrating.

Enkele andere aandachtspunten zijn ten slotte:

- Bestaat de indruk, dat criminaliteit en vandalisme mogelijkereis verband houden met de aanwezigheid van scholen in de buurt, overleg dan met de schoolleiding. Informatielessen op scholen kunnen nuttig zijn.
- In overleg met de politie kan er bezien worden of er alternatieve straffen mogelijk zijn die verband houden met de gepleegde delicten.
- Het direct verwijderen van bekladdingen op muren vermindert de aantrekkingskracht voor de makers van nieuwe 'verfraaiingen'. Meer informatie over gevelreiniging is te vinden in twee andere SBR-publicaties over dit on-

Afvalcontainers niet onder een luifel plaatsen



derwerp: publikatie nr. 104 en nr. 152.

- Vuilcontainers moeten goed afsluitbaar zijn; afval eromheen dient zo snel mogelijk opgeruimd te worden.
- De schade door ruitbreuk kan beperkt worden door een grote serie verschillende maatregelen. We verwijzen hiervoor naar hoofdstuk 5 van deel 3.
- Maak met de politie de afspraak dat elke onregelmatigheid gerapporteerd zal worden. Het ontwerpen van een klein standaard-meldingskaartje is aan te bevelen.

Uitgebreidere informatie over vandalisme is te verkrijgen bij de volgende instellingen (zie ook bijlage 2: Organisaties en instellingen):

- Nationaal Brandpreventie Instituut;
- Technisch Bureau ter Bevordering van Schadepreventie (TBBS);
- Landelijk Bureau Voorkoming Misdrijven (of lokale politie ambtenaren Voorkoming Misdrijven).

Tot slot wijzen we nogmaals op het tweede deel in deze serie Beveiliging van Gebouwen (Meergezinswoningen) waarin veel uitgebreider stilgestaan wordt bij vandalisme(preventie).

- Architect, de: Themanummer over bedrijfsgebouwen, nr. 33, 1988.
- Bleker, B.: Technologische ontwikkelingen relativeren belang gebouw. In: *de Architect* (themanummer over Bedrijfsgebouwen), pagina 58-61, nr. 33, 1988.
- Dijk, A. G. van, en P. M. Savornin Lohman: *Diefstal en vernieling op de bouwplaats, een oriënterend onderzoek onder aannemers*. Bureau Criminaliteitspreventie, Amsterdam, december 1985.
- Dijk, J. J. M. van, en A. Röell: Criminaliteit in tal en last. Een raming van de schade- en kostenposten in verband met criminaliteit. In: *Justitiële verkenningen*, deel 2, 1988, pag. 7-33.
- Green, G.: *Introduction to security* (fourth edition; revised by R. J. Fischer). Buttersworth, Boston 1987.
- Healy, R. J., en T. J. Walsh: *Industrial security management*. American Management Association, New York 1971.
- Heuvel, A. L. W. C. M. van den, en W. D. van der Valk: *Winkelcriminaliteit in het midden- en kleinbedrijf*. Economisch Instituut voor het midden- en kleinbedrijf, Zoetermeer, augustus 1986.
- Hogenbirk, J., en A. Loggers: zie onder Zadelhoff.
- Hope, T. J.: *Burglary in Schools: The Prospects for Prevention*. Research and Planning Unit Paper nr. 11, Home Office, London 1982.
- NBF: *Een brandveilig gebouw bouwen*. (Verkrijgbaar bij de afdelingen brandpreventie van de brandweer van de gemeenten Amsterdam, Rotterdam en 's-Gravenhage. In deze serie is inmiddels ook verschenen: 'Een brandveilig gebouw installeren' en 'Een brandveilig gebouw gebruiken'.)
- Regterschot, J.: *Facility management (Het professioneel besturen van de kantoorhuisvesting)*. Kluwer, Deventer 1988.
- SBR: *Een brandveilig gebouw ontwerpen*, publikatie 91. Stichting Bouwresearch Rotterdam.
- SBR: *Gevelreiniging in de praktijk*, publikatie 104. Stichting Bouwresearch Rotterdam.
- SBR: *Gevelreiniging: reinigend effect en schade met chemische middelen en gritstralen*, publikatie 152. Stichting Bouwresearch Rotterdam.
- Rompelman, D. A., en E. A. van Deelen: De commerciële vastgoedmarkt in 1988. In: *VastGoedMarkt* nr. 1, januari 1989, pagina 1-9.
- SEC (kwartaalblad over samenleving en criminaliteit): Kleine criminaliteit wat kost dat? (vraagtekens bij kosten van vandalisme voor bedrijfsleven), *SEC januari 1989*, 3e jaargang nr. 1 pagina 16/17.
- SMP (Stichting Maatschappij en Politie): *Naar een economische benadering van criminaliteit en veiligheidszorg* (Oriënterend onderzoek uitgevoerd in opdracht van de Stichting Maatschappij en Politie door de stichting Het Nederlands Economisch Instituut), B. Verhoef, A. Verster en L. Klaassen, Dordrecht, oktober 1988.
- Staal, G.: *Bouw heer en meester, de architectuur van kantoorgebouwen*, 1987.
- TBBS: rapport nr. 0046R: *Nooddeuren*. Baarn, juli 1987.
- Tien, J. M., en M. F. Cahn: The commercial security field test program: A systemic evaluation of security surveys in Denver, St Louis and Long Beach. In: D. Rosenbaum (1986), *Community crime prevention*. Newbury Park: Sage.

VNG: *In de vernieling. Een onderzoek naar omvang, frequentie en kosten van vernieling van gemeentelijk eigendom*, VNG, 's-Gravenhage, oktober 1984.

VNO/NCW: *Handleiding beveiliging* (3e druk). VNO/NCW, 's-Gravenhage, oktober 1984.

Zadelhoff Makelaars / Rijksuniversiteit Utrecht (Faculteit der Ruimtelijke Wetenschappen Vakgroep Toegepaste Geografie en Ruimtelijke Planning): *Dynamische ontwikkeling op de markt voor kantoor- en bedrijfsruimte in Nederland in de jaren 1983–1988*. Zadelhoff Makelaars, Amsterdam, oktober 1988.

INHOUDSOPGAVEN DEEL 1, 2, 3 EN 5

0:11 1

■ Deel 1 – EENGEZINSWONINGEN

In de serie Beveiliging van gebouwen

Woord vooraf

Samenvatting

Summary

1 Inleiding

Het probleem

Leeswijzer

Begripsafbakening

Inbraakpreventie: wat wordt er
(nog steeds niet) aan gedaan?

2 Achtergronden van inbraak

Omschrijving

Omvang

Daders

Tijdstip en modus operandi

Spreiding van inbraken over
Nederland

Spreiding van inbraken over stad of
gemeente

Spreiding van inbraken over een
buurt/straat/huizenblok

Inbraak en preventie

3 Bouwtechnisch beveiligen

Omschrijving

Keuze-aspecten van kozijnen,
ramen en deuren

Hang- en sluitwerk

Deuren

– voordeuren

- overige buitendeuren, zoals

keuken-, terras- en balkondeuren

- enkelvoudige deuren

- dubbele deuren

– schuifdeuren

– deuren tussen de woning en
aangebouwde bijgebouwen

- aansluitende constructies

Ramen

Andere constructies (daken,
dakramen, lichtkoepels, enz.)

Onderlinge samenhang,
projectering en bevestiging

Kostenaspecten

Verlichting

4 Diversen

Alarmsystemen

Herkenbaarheid en verkrijgbaar-
heid van inbraakveilig hang- en
sluitwerk

Risicoklassesysteem

Verzekeringen

Voorraad, kwaliteit en trends van
woningen

Beveiligingsplan

Checklist

Literatuur

Bijlage

Organisaties en instellingen

Colofon

■ Deel 2 – MEERGEZINSWONINGEN

In de serie Beveiliging van gebouwen

Woord vooraf

Samenvatting

Summary

1 Inleiding

Het probleem
Risico's voor de meergezinswoning:
vandalisme en inbraak
Techno-preventie van vandalisme:
veel specialisten, weinig overzicht
Leeswijzer

2 Achtergronden van vandalisme

Omschrijving
Ontwikkeling, omvang en schade
Daders
Spreiding van vandalisme over
Nederland
Spreiding van vandalisme over de
stad/gemeente
Kenmerken van
vandalismegevoelige plekken
– buiten woongebouwen
– in en aan woongebouwen
Routes
Samenvatting: waar komt
vandalisme (meer) voor?

3 Vandalismepreventie: strategieën en ervaringen

Inleiding
Tien strategieën
Vandalismepreventie: beheerders
aan het woord
– algemeen
– stedenbouwkundig niveau
– niveau hoofdopzet
– niveau detaillering
Conclusies

4 De omgeving van het gebouw

Inleiding
Risicogebieden
– speelplaatsen

– groenstroken
– vuilnisverzamelplaatsen
– garages
Objecten en materialen
– verlichting
– afrasteringen en hekwerken
– straatnaamborden, bewegwij-
zering en dergelijke

5 Het gebouw

Inleiding
Risicoplekken
– de entree
– bergingen
– liften
– platte daken
Vernielde objecten
– wanden
– vloeren en plafonds
– entreedeur
– ramen en glas
– kozijnen
– brievenbussen, belcensborden
en spreekinstallaties
– leidingen en verlichting
– roosters en bouwbeslag

6 Inbraakbeveiliging

Inleiding
Voordeur
Bergingen
Compartimenteren

7 Checklist en aandachtspunten

Literatuur

Bijlagen

1 Inhoudsopgave deel 1

2 Organisaties en instellingen

Colofon

■ Deel 3 – WINKELS

In de serie Beveiliging van gebouwen

Woord vooraf

Samenvatting

Summary

1 Inleiding

Het probleem
Risico's voor winkels

2 Winkels en criminaliteit

Criminaliteit en lekkage
Het EIM-onderzoek
Inbraak
– inleiding
– omvang en ontwikkeling
– materiële schade
– extra verzekeringsvoorwaarden

3 Commerciële uitgangspunten

Inleiding
Belangrijke functies van het winkelinterieur
De luifel
De etalage
De ingang
Slotopmerking

4 Het beveiligingsplan

Inleiding
De 'beveiligingsvaardige'
ontwerper: vier aandachtspunten
De PIVA-ALRE-theorie
Beveiligingsmaatregelen en hun onderlinge samenhang
Slotopmerkingen

5 Bouwtechnisch beveiligen

De pui
– de ingangspartij
– het kozijn
– het glas
– de glasafscherming
– obstakels in en voor de pui
De zij- en achterkant
– ramen en deuren

– vluchtdeuren

Aangrenzende ruimten van de winkel

– aangebouwde bijgebouwen
– kelders en kruipruimten
– ruimten boven plafonds
– bovenwoningen
– trappehuizen en leidingschachten
– daken

Terrein; afscheiding en verlichting

Inbraakwerende compartimenten

Geldzaken

– brandkasten en kluizen
– kassier- en geldtelruimte
– intern en extern geldtransport

6 Het stadsschoon en de regels

Het probleem van de rolluiken
Voorstanders
Tegenstanders
De rol van ontwerpers
Slotopmerkingen

7 Wonen boven winkels

Inleiding
Helpt wonen boven winkels echt tegen inbraak?
Problemen
Ontwerpvoorbeelden
Ontwerpvoorbeelden
nieuwbouw/renovatie
Bestaande bebouwing:
het voorbeeld Haarlem

8 Collectieve oplossingen

Wat kunnen winkeliers collectief aanpakken?
Voor- en nadelen collectieve aanpak
De rol van ontwerpers
Uitwerking
Slotopmerkingen

Literatuur

Bijlagen

(zie verder)

(vervolg inhoudsopgave deel 3)

Bijlagen

- 1 Inhoudsopgave deel 1 en 2**
- 2 Organisaties en instellingen**
- 3 Winkelvoorraad**
- 4 Tabellen inbraak, vandalisme en intimidatie**
- 5 Verzekeringsvoorwaarden**
- 6 Winkeldiefstal**
- 7 Vandalisme en brandstichting**
- 8 Elektronische beveiliging**
- 9 Prijsidee**
- 10 Winkelinterieur**

Colofon

■ Deel 5 – BEDRIJFSGEBOUWEN / TERREINEN

In de serie Beveiliging van gebouwen

Woord vooraf

Samenvatting

Summary

1 Inleiding

Algemeen
Definitie bedrijfsgebouwen
Gebouwtypen
Voorraad, trends, prijs en afnemers

2 Risico's

Algemeen
Vandalisme, inbraak, diefstal en brandstichting
Vandalisme
Inbraak
Brandstichting
Enkele schadevoorbeelden

3 Risicobeheer en risicobeoordeling

Algemeen
Risicobeheer
Ruimte-risico-inschattingsmodel (RRIM)

4 Beveiliging en bewaking

Algemeen
Fysieke zones
Bewakingssystemen
■ toegangscontrole
– waarschuwingssysteem
– opvolging
Recente ontwikkelingen

5 Het gebouw

Algemeen
Gevels, kozijnen, ramen en deuren
■ gevels
– kozijnen, ramen en deuren
– bedrijfsdeuren
Hang- en sluitwerk
Glas en glasafscherming
– glas
– glasafscherming

– kogelwering
Daken en vluchtwegen
– lichtkoepels en dergelijke
– vluchtwegen
Inbraaksignaleringsystemen
Functie
– werking
– installatie
■ de bouwkundig ontwerper

6 Het terrein

Algemeen
Stedebouwkundige opzet
bedrijfsverzamelterrein
– verkoopargumenten
– criminaliteitspreventieve aandachtspunten
– verdere aandachtspunten
Individuele terreinen

7 Terreinafscheiding

Algemeen
Technische afscheidingen
– hekwerken
– muren
– schuttingen
– puntdraadafscheidingen
Natuurlijke afscheidingen
– wallen
– grachten
– sloten
– hagen en struiken

8 Toegangsbeveiliging

Algemeen
Toegangscontrole
– toegangscontrole aan de poort
– poortuitvoeringen
– toegangsbeveiliging voertuigen

9 Beveiligingsverlichting

Algemeen
Enkele algemene aspecten van licht en criminaliteit

(zie verder)

(vervolg inhoudsopgave deel 5)

- onderzoek naar effecten
- applicatie-onderzoek
- De toepassing van beveiligingsverlichting
 - afstemmen op de omstandigheden
 - lichtbehoefte
- Bedrijfsgebouwen en -terreinen
- Speciale toepassingen
- Installatie
- Beveiligingsverlichting bij toepassing van gesloten televisiecircuits
 - lichtinvalshoek
 - verblinding
 - keuze lichtsterkte objectief en verlichtingssterkte
 - lichtkleur
 - berekening verlichtingsvoorstel
- 10 Gesloten televisiesystemen**
 - Algemeen
 - Televisiecamera
 - Camerabehuizing
 - Beeldoverdracht
 - Monitor
 - Beeldpresentatie
 - Videorecorders
 - Systeemintegratie
 - Buitenverlichting en CCTV
 - Observatie van terrein en afscheiding
 - Ontwerp en keuze van apparatuur
- 11 terreindetectiesystemen**
 - Algemeen
 - De mogelijkheden
 - De systemen
 - op, in en boven het hekwerk
 - boven de grond
 - in de grond
 - Nodeloos alarm
 - Aanschaf en installatie van het systeem

Bijlagen

- 1 Inhoudsopgaven deel 1, 2, 3 en 4**
- 2 Organisaties en instellingen**
- 3 Risicoklassesysteem verzekeraars**
 - Inbraakgevoeligheid meten
 - Bepaling van het aantal risicopunten
- 4 Bewakingspersoneel**
 - Organisatie
 - Bijzondere eisen voor beveiligingspersoneel
 - Bevoegdheden bewakingspersoneel
- 5 Veiligheid van gebouwen: eisen van de arbeidsinspectie**
 - Deuren en beweegbare hekken
 - Bouw en inrichting van bedrijfsruimten
 - Deurtypen
- 6 Licht**
 - Licht en oogtaak
 - licht
 - oogtaak
 - Lichtbronnen
 - soorten
 - rendementsvergelijking
 - gloeilamp
 - halogeenlamp
 - hogedruk-kwiklamp
 - fluorescentielamp
 - hogedruk-natriumlamp
 - lagedruk-natriumlamp
 - Armaturen
 - Exploitatieberekening

Colofon

~~~~~

**Stichting Kwaliteitscentrum  
Gevelelementen  
Bredewater 20  
Postbus 190  
2700 AD Zoetermeer  
tel. 079 – 51 18 03**



**SVB**

Stichting Veiligheidsbeglazing  
Groningenweg 6  
2803 PV Gouda  
tel. 0 18 20 – 3 71 21

**Stichting Slotencertificaat**

Postbus 54,  
3740 AB Baarn  
tel. 0 21 54 – 1 64 41

**TBBS**

Bureau voor Schadepreventie  
Eemnesserweg 56  
Postbus 54  
3740 AB Baarn  
tel. 02154 – 1 64 41

**UNETO**

Unie van elektrotechnische  
ondernemers  
Parkstraat 32  
Postbus 85.546  
2508 CE Den Haag  
tel. 070 – 62 44 91

**VHS**

Vereniging Fabrikanten Hang- en  
Sluitwerk  
Postbus 190  
2700 AD Zoetermeer  
tel. 079 – 53 11 00

**VMR**

Vereniging van Metalen  
Ramenfabrikanten  
Bredewater 20  
Postbus 190  
2700 AD Zoetermeer  
tel. 079 – 53 11 00

**VKG**

Vereniging Kunststof  
Gevelementenfabrikanten  
Bredewater 20  
Postbus 190  
2700 AD Zoetermeer  
tel. 079 – 53 11 00

**VNO**

Verbond van Nederlandse  
Ondernemingen  
Postbus 93.093  
2509 AB Den Haag  
tel. 070 – 49 73 73

## **Uitgever**

Stichting Bouwresearch, Rotterdam

## **Productie**

Bureau Criminaliteitspreventie, Amsterdam

P. van Soomeren, H. Stienstra, met medewerking van M. van Putten

## **Vormgeving**

R. Heerema, Bureau Criminaliteitspreventie, Amsterdam

Sytske A. Wieringa, Groningen

## **Omslag en illustraties**

R. Heerema, Bureau Criminaliteitspreventie, Amsterdam

## **Foto's met dank aan**

Articolor Fotografie, Driebergen

Boon, Edam

Cardkey Systems Limited, Berks (Engeland)

Double Design, Zeist

Hageman, Raamsdonksveer

Otto Lampertz GmbH & Co, Betzdorf (W-Duitsland)

Laurens Janus, Oostenhout

Martens Brandkasten, Doetinchem

M. van Putten, Amsterdam

Radio Holland Group, Amsterdam

Rofoto, Rotterdam

Schlage Electronics

Sellox, IJsselstein

H. Stienstra, Putten

Sytske A. Wieringa, Groningen

Words & Pictures, Slough (Engeland)

## **Studiecommissie C-40, Beveiliging gebouwen**

P. A. v.d. Heiden, voorzitter; ABN, afdeling Bouwzaken

C. M. Faling, architect

T. Jung, Jung Security BV

B. F. M. van Slobbe, AMEV Vastgoed BV

A. Stöver, Centrale Directie PTT

P. Schurink, studietoördinator Stichting Bouwresearch

R. Meijer, Bureau Landelijk Coördinator Voorkoming Misdrijven

P. van Soomeren, Bureau Criminaliteitspreventie

H. Stienstra, Bureau Criminaliteitspreventie

## *Overige relevante publikaties van Stichting Bouwresearch*

- \* In relatie tot het onderwerp van deze publikatie is/zijn reeds verschenen (of is/zijn binnenkort beschikbaar) SBR-publikatie(s):
  - nr. 160 Beveiliging van gebouwen;  
deel 1: Eengezinswoningen.
  - nr. 170 Beveiliging van gebouwen;  
deel 2: Meergezinswoningen.
  - nr. 180 Beveiliging van gebouwen;  
deel 3: Winkels.
  - nr. 184 Beveiliging van vluchtwegen.
- \* De nieuwste uitgaven van SBR worden altijd besproken in het vier maal per jaar verschijnende SPEURBERICHT. Neem een (gratis) abonnement als u het nog niet krijgt, het bevat tevens een lijst van alle SBR-publikaties en SBR-computerprogramma's.
- \* Beter nog: neem een abonnement op de SBR-publikaties. U krijgt dan iedere schriftelijke uitgave (publikatie, Speurbericht, jaarverslag, aankondiging van Technische Dagen) direct na verschijning toegezonden. Bovendien krijgt u 15 procent korting op de verkoopprijs van de door SBR ontwikkelde computerprogramma's die overigens apart moeten worden besteld. De prijs van dit publikatie-abonnement zal u meevallen.

*Inlichtingen over SBR-publikaties, het abonnement daarop en/of toezending van het Speurbericht bij:*

Stichting Bouwresearch  
Postbus 20740  
3001 JA ROTTERDAM  
Telefoon (010) 412 35 28 / 411 72 76  
Telefax (010) 413 01 75