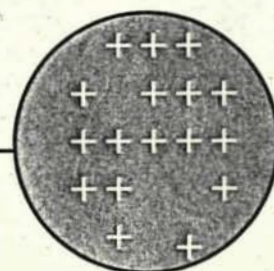


Veiligheidsbeleid

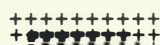
+

+

+

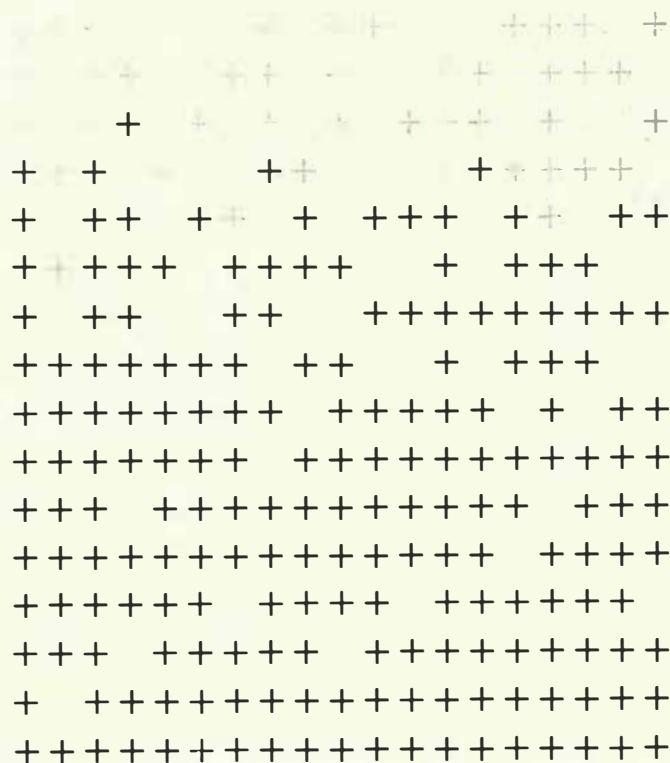


Handboek veilige
zorginstellingen



95/71

nr.enlandse Zaken



Handboek veilige Zorginstellingen

Den Haag, augustus 1995
DamhuisElshoutVerschure
Van Dijk, Van Soomeren en Partners

Inhoudsopgave

Voorwoord
Samenvatting

Inleiding 1

Deel I De huidige stand van zaken

1 *De problemen* 2

1.1 Typen onveiligheid 2

1.2 Risico's 4

1.2.1 Risicovolle lokaties 4

1.2.2 Risicovergrotenende factoren 5

1.3 Gevolgen van onveiligheid 8

2 *De beveiliging* 10

2.1 Het beveiligingsniveau van zorginstellingen:
ideaal en werkelijkheid 10

2.2 Het verband tussen beveiliging, arbo-zorg en
kwaliteitszorg: op zoek naar synergie 12

2.3 Conclusies 14

Deel II De weg naar integrale beveiliging 16

3 *Het preventiewiel* 16

3.1 Het beveiligingsbeleid 18

3.2 De beveiligingsorganisatie 18

3.2.1 De beveiligingsstructuur 18

3.2.2 De beveiligingsprocessen 19

3.3 Technische voorzieningen 21

3.4 Cultuur 22

3.4.1 Deskundigheidsbevordering 22

3.4.2 Een preventiehouding 23

4 *Het ontwikkelen van een beveiligingssysteem in een zorginstelling* 24

4.1 Fasen in het opzetten van een beveiligingssysteem 24

4.2 De voorbereidende fase 25

4.2.1 Het verkrijgen van draagvlak 25

4.2.2 Het opzetten van een projectorganisatie beveiliging 27

4.2.3 Het maken van een projectplan 30

4.2.4 De formele vaststelling van het plan van aanpak 34

4.3 De analysefase: het beveiligingsonderzoek 35

4.3.1 De incidentenregistratie 35

4.3.2 De kleurenmethode 37

4.3.3 De personeelsenquête 39

4.3.4 De security audit 41

4.4 De beleidsfase 44

4.4.1	Het vaststellen van maatregelen en middelen	44
4.4.2	Het schrijven van een beveiligingsbeleidsplan	44
4.5	De uitvoerings- en evaluatiefase	46

Bijlagen: Instrumenten

1	Voorbeeld van een projectplan
2	Voorbeeld van een dagprogramma security audit en observatiechecklist
3	De kleurenmethode
4	De personeelsenquête
5	Vragenlijst preventiewiel en security audit
6	Voorbeeld incidentmeldingsformulier
7	Voorbeeld communicatieplan
8	Overzicht Vetron beveiligingsinstituten en -trainingen
9	Aandachtspunten bij de aanpak van agressie en geweld
10	Aandachtspunten bij bouwkundige en elektronische beveiliging
11	Samenvatting brandbeveiligingsconcept gezondheidszorggebouwen

Literatuur

Voorwoord

5

Voor u ligt het Handboek Beveiliging Zorginstellingen. Dit handboek is bedoeld voor managers van zorginstellingen en andere functionarissen die belast zijn met de beveiliging van de instelling. In dit handboek worden handvatten gegeven om te komen tot een integraal systeem van beveiliging binnen zorginstellingen.

De volgende functionarissen hebben een bijdrage geleverd aan de totstandkoming van deze handleiding:

- de heer C.F. Busschers,
coördinator van het project "Veiligheid, ons een zorg!",
Politie Regio Twente
- mevrouw J.A.M. Eertman,
project-assistent, Politie Regio Twente
- de heer J.A. Eshuis
Streekziekenhuis Midden-Twente
- de heer H. Gerritsen
Medisch Spectrum Twente
- de heer A. Maneschijn
Revalidatiecentrum Het Roessingh
- de heer B. Mues
Revalidatiecentrum Het Roessingh
- de heer D.P. Wijnen
Twents Psychiatrisch Ziekenhuis
- mevrouw Y. Beerning
Twenteborg Ziekenhuis
- mevrouw A.E. Osse
coördinator van het project "Sociale Veiligheid in en rond zorginstellingen Flevoland"
- mevrouw C.E.M. Brouwer
projectcoördinator ziekenhuisproject Utrecht.

Dit handboek is in opdracht van het projectbureau "Veiligheid, ons een zorg", en het Ministerie van Justitie, Hoofdafdeling Criminaliteitspreventie, onder verantwoordelijkheid van een begeleidingscommissie, opgesteld door DamhuisElshoutVerschure, organisatie-adviseurs te 's Hertogenbosch en Van Dijk, Van Soomeren en Partners te Amsterdam. In een later stadium is het project overgegaan naar het Ministerie van Binnenlandse Zaken.

De begeleidingscommissie bestond uit de volgende personen:

- De heer N. van Leeuwen
Ziekenhuis Leyenburg, Den Haag
- de heer P. van Soomeren
Van Dijk, Van Soomeren en Partners
- de heer A. Trip
Ministerie van Volksgezondheid, Welzijn en Sport
- de heer K. Verschure
DamhuisElshoutVerschure
- de heer A. Voermans
Ministerie van Binnenlandse Zaken
- de heer M. Vroombout
Regiopolitie Rotterdam Rijnmond

Wat kunt u in dit handboek vinden?

7

Het doel van dit Handboek Beveiliging Zorginstellingen is om managers kennis en instrumenten aan te reiken om de beveiliging van hun zorginstelling op een hoger plan te tillen. Op dit moment blijken de meeste zorginstellingen helaas nog in de zogenaamde 'bewakersfase' te vertoeven: de aandacht voor beveiliging blijft grotendeels beperkt tot het installeren van technische beveiligingsmiddelen en het aanstellen van beveiligingsfunctionarissen, die "het verder maar moeten regelen". Beveiliging wordt als een apart vakgebied beschouwd dat los van de lijn en van de andere zorggebieden functioneert. De noodzaak voor een meer integrale benadering van beveiliging van zorginstellingen neemt echter toe. Enerzijds omdat werkgevers sinds de invoering van de nieuwe arbo-wet wettelijk verplicht zijn gesteld om minimaal een deel van de onveiligheid (sexuele intimidatie, agressie en geweld op de werkplek) integraal aan te pakken, anderzijds omdat het bewustzijn groeit dat onveiligheid veel schade en persoonlijk leed veroorzaakt.

Het dichten van de toenemende kloof tussen het bestaande en het gewenste beveiligingsniveau is echter niet eenvoudig. Om te beginnen is er voor het structureel verbeteren van beveiliging **draagvlak bij het management** nodig. Verder zijn er de nodige **kennis en instrumenten** nodig om stapsgewijs een integrale beveiliging te kunnen ontwikkelen.

Deel I van het handboek verschaft het management inzicht in de noodzaak van een integrale aanpak van beveiliging. In hoofdstuk 1 van dit handboek wordt uiteengezet van welke beveiligingsproblemen zorginstellingen zoal last kunnen krijgen, welke risico-factoren hierbij een rol spelen en welke gevolgen criminaliteit en onveiligheidsgevoelens hebben voor de instelling. Hierbij wordt benadrukt dat onveiligheid niet alleen directe materiële schade tot gevolg heeft, maar ook een negatief effect kan hebben op de kwaliteitszorg en de arbeidsomstandigheden binnen de instelling. In hoofdstuk 2 wordt uiteengezet dat het een gemiste kans is om beveiliging los te koppelen van de kwaliteitszorg en de arbo-zorg. Het is van belang dat het management gaat inzien dat er overlappingen bestaan tussen kwaliteitszorg, arbo-zorg en beveiliging en dat er bij het integraal aanpakken van beveiliging gebruik kan worden gemaakt van de synergie-mogelijkheden die deze overlappingen bieden. Het benutten van deze synergie-mogelijkheden kan namelijk alle drie zorggebieden ten goede komen en de instelling in totaliteit winst op leveren doordat er efficiënter en effectiever met menskracht en middelen wordt omgegaan.

De benodigde kennis en instrumenten voor het stapsgewijs ontwikkelen van integrale beveiliging zijn in deel II en in de bijlagen van het handboek te vinden. Deze instrumenten zijn in de praktijk in een tiental zorginstellingen uitgetest en bleken daar duidelijk vruchten af te werpen. In hoofdstuk 3 wordt eerst beschreven hoe een integraal beveiligingssysteem er uit ziet. In hoofdstuk 4 wordt vervolgens stap voor stap uiteengezet hoe een structurele beveiligingsaanpak gestalte kan krijgen. Hierbij worden de volgende fasen onderscheiden:

- 1 De voorbereidende fase, waarin draagvlak wordt verkregen voor het opzetten van een structurele aanpak van beveiliging en waarin een projectplan van aanpak wordt ontwikkeld.
- 2 De analyse-fase, waarin met behulp van instrumenten als de incidentenregistratie, de kleurenmethode, de personeelsenquête en de security audit een beeld kan worden verkregen van de beveiligingsproblematiek in de instelling.
- 3 De beleidsfase, waarin maatregelen en middelen worden vastgesteld en het beveiligingsplan wordt geschreven.
- 4 De uitvoerings- en evaluatiefase, waarin de beschreven maatregelen worden uitgevoerd en op grond van evaluatie eventueel later worden bijgestuurd.

Er is nauwkeurig beschreven hoe deze verschillende fasen in de praktijk ingevuld kunnen worden, zodat het handboek een goed handvat biedt voor instellingen die een structurele beveiligingsaanpak willen ontwikkelen. In de bijlagen zijn de bij het stappenplan behorende instrumenten opgenomen, die direct toepasbaar zijn in zorginstellingen, zodat elke instelling daar in de praktijk zelf mee kan gaan werken.

Al met al biedt het handboek geen pakkende oplossingen, maar verschaft het wel kennis, concrete richtlijnen en instrumenten. Het is praktisch van opzet en nodigt uit tot handelen. In het belang van de klanten, het personeel en de instellingen zelf.

Inleiding

Een patiënt mist sieraden, een medewerker zijn portefeuille en op de parkeerplaats is uit de auto van een bezoeker een radio ontvreemd. Ook al varieert het risico per type instelling, feit is dat alle zorginstellingen te maken kunnen krijgen met onveiligheidsproblemen. Het analyseren en aanpakken van deze problemen kan voor al deze instellingen op een in hoofdlijnen vergelijkbare manier plaatsvinden.

Dit handboek is daarom ook gericht op alle zorginstellingen, dus:

- algemene ziekenhuizen;
- psychiatrische en andere gespecialiseerde ziekenhuizen;
- psychiatrische inrichtingen;
- verzorgingstehuizen.

Het management van een zorginstelling is er zich in het algemeen wel bewust van dat het 'iets' aan beveiliging moet doen. Door gebrek aan kennis en inzicht worden er echter meestal maatregelen getroffen, die bij nadere beschouwing niet het meest effectief en efficiënt blijken te zijn. Feitelijk wordt hierdoor geld verspild en worden mensen en middelen niet efficiënt ingezet. Bovendien worden de onveiligheidsrisico's niet effectief aangepakt, waardoor de negatieve gevolgen van onveiligheid groter zijn dan nodig is. Aldus kan niet alleen de materiële schade oplopen tot onprettige proporties, maar kunnen ook de gevoelens van onveiligheid van werknemers, bezoekers en patiënten toenemen en kan de werksfeer en de kwaliteit van de dienstverlening geschaad worden.

Redenen genoeg om de beveiliging in en rond een zorginstelling serieus te nemen. Een extra reden vormt bovendien nog de recente wijziging van de Arbo-wet, waardoor werkgevers verplicht worden om agressie en (seksueel) geweld op de werkvloer tegen te gaan. Aan deze vormen van onveiligheid moet dus meer en structureler aandacht worden besteed dan voorheen. Dit betekent dat een gestructureerde aanpak van onveiligheid niet alleen wenselijk is, maar op onderdelen ook wettelijk verplicht. Het doel van dit handboek is om zorginstellingen te helpen hun beveiliging op een hoger plan te brengen. Het biedt geen panklare oplossingen, maar verschaft het management van zorginstellingen wel kennis, concrete richtlijnen en instrumenten om de beveiliging structureel vorm te geven en te verbeteren. Het is praktisch van opzet en heeft reeds z'n nut bewezen: de in dit handboek geschetste integrale aanpak van beveiliging is namelijk al in een tiental zorginstellingen in praktijk gebracht¹ en bleek duidelijk vruchten af te werpen.

We hopen daarom dat u dit handboek niet alleen zult lezen, maar dat het u ook zal aanzetten tot handelen. In het belang van uw klanten, uw personeel en de instelling zelf.

¹ Zie noten pagina 109

Deel I De huidige stand van zaken

11

1 De problemen

1.1 Typen onveiligheid

Bij het begrip onveiligheid dient onderscheid gemaakt te worden tussen daadwerkelijk plaatsvindende onveiligheid en subjectieve gevoelens van onveiligheid. Het aspect brandveiligheid zal in dit hoofdstuk niet nader worden beschouwd. De brandveiligheidsvisie van zorginstellingen staat reeds beschreven in een door het Ministerie van Binnenlandse Zaken uitgegeven boekwerk 'brandbeveiligingsconcept gezondheidszorg gebouwen' (bestelnummer 76109430112, Logistiek Centrum Ministerie van Binnenlandse Zaken, telefax: 079 - 3614986). In bijlage II van dat boekwerk is een beknopte samenvatting opgenomen. In het navolgende gaan we nader in op die vormen van onveiligheid die veroorzaakt worden door criminaliteit.

Criminaliteit

Zorginstellingen kunnen te maken krijgen met de volgende verschijningsvormen van criminaliteit:

- vandalisme/vernieling;
- eenvoudige diefstal;
- diefstal met braak (inbraak);
- diefstal met geweld (beroving, overval);
- fraude/verduistering;
- computercriminaliteit;
- brandstichting;
- bedreiging, agressie en intimidatie;
- zedendelicten (ongewenste intimiteiten, seksuele intimidatie, aanranding, verkrachting);
- (zware) mishandeling, moord en doodslag;
- bomdreiging/ontvoering/chantage/terrorisme.

Sommige verschijningsvormen zullen zelden of nooit voorkomen (moord en doodslag, bomaanslagen etc.), terwijl andere aan de orde van de dag zijn.

Vooraf diefstal en agressie zijn in veel zorginstellingen frequent optredende verschijnselen².

Er kan onderscheid gemaakt worden tussen externe en interne criminaliteit.

Externe criminaliteit is criminaliteit die veroorzaakt wordt door daders van buitenaf,

² Zie noten pagina 109

die niet werken in of rondom de zorginstelling. De preventie van externe criminaliteit richt zich met name op:

- 1 het voorkomen van inbraak;
- 2 het weren van mensen die niets in de instelling te zoeken hebben;
- 3 het zorgen voor een veilige omgeving (parkeerterrein, loop- en fietsroutes e.d.);
- 4 het voorkomen van diefstal door externen (klanten, "rondlopers" e.d.).

Bij interne criminaliteit is inbraak of insluiping niet nodig: de dader bevindt zich in dit geval reeds legitiem in het gebouw als werknemer (van het ziekenhuis of van ondersteunende diensten).

12

Bij de beveiliging wordt de aandacht vaak veel te veel gericht op daders van buitenaf. Een instelling geeft niet graag openlijk toe dat de werknemers zich ook regelmatig schuldig maken aan criminaliteit en beleidsmatig wordt aan dit probleem dan ook weinig aandacht besteed. Bovendien is het voorkomen van interne criminaliteit lastig. De daders zijn immers afkomstig uit de eigen gelederen en kunnen daarom niet geweerd worden. Toch kan er wel degelijk iets aan gedaan worden. Met name organisatorische maatregelen, interne bouwkundige maatregelen (compartimentering, zonering) en het nauwgezet selecteren van betrouwbaar personeel kunnen hier vruchten afwerpen. Aangezien het vermoeden bestaat dat een aanzienlijk deel van de criminaliteit ook gepleegd wordt door interne daders, verdient de preventie hiervan zeker de nodige aandacht. Verschillende maatregelen die gericht zijn op het voorkomen van interne criminaliteit zullen overigens veelal ook het plegen van externe criminaliteit bemoeilijken.

In een verzorgingstehuis worden in toenemende mate waardevolle spullen ontvreemd. De daders hebben het vooral gemunt op sieraden en audio- en video-apparatuur. Dit levert aardig wat schade op en de bewoners gaan zich ook steeds onveiliger voelen. Er wordt daarom extra budget vrijgemaakt (de aanschaf van de nieuwe computer moet nog maar even wachten) om toegangsdeuren en ramen te voorzien van beter hang- en sluitwerk en baliemedewerkers worden geïnstrueerd om extra alert te zijn op mensen die niets in de instelling te zoeken hebben. Dit blijkt echter niets op te leveren: er blijven spullen verdwijnen. Na enkele maanden wordt de dader bij toeval op heterdaad betrapt. Het blijkt een werknemer te zijn met gokschulden. Bij navraag bleek hij zich op z'n vorige werkplek ook schuldig te hebben gemaakt aan diefstal.

Onveiligheidsgevoelens

Zowel patiënten, bezoekers als het personeel van zorginstellingen kunnen kampen met onveiligheidsgevoelens. Een indicatie voor de omvang van dit probleem vormt de uitkomst van een landelijk onderzoek waaruit blijkt dat 63% van de medewerkers van ziekenhuizen zich regelmatig onveilig voelt³.

Een wijd verbreid misverstand is dat door het bestrijden van criminaliteit de onveiligheidsgevoelens vanzelf zouden afnemen. Onveiligheidsgevoelens blijken echter door een complex van factoren veroorzaakt te worden, waar criminaliteit wel deel van uitmaakt maar in veel gevallen niet allesbepalend is. Het bestrijden van onveiligheidsgevoelens verdient daarom aparte aandacht, niet in de laatste plaats omdat zulke gevoelens verstrekkende negatieve consequenties kunnen hebben voor de betrokkenen. Wel dient de aanpak van onveiligheidsgevoelens hand in hand te gaan met het bestrijden van de daadwerkelijk optredende criminaliteit: voorkomen moet worden dat er een schijn van veiligheid wordt gecreëerd in een onveilige situatie.

³ Zie noten pagina 109

Uit een enquête onder verpleegsters bleek dat een ruime meerderheid van hen zich erg onveilig voelde op de fietsroute van en naar het ziekenhuis. Er liep maar één fietspad van het ziekenhuis naar de belendende woonwijk en dit pad liep door een donker, verlaten park. De meeste verpleegsters durfden daarom niet op de fiets naar hun werk te komen, maar namen de auto. Dit vormde voor de instelling reden om in samenwerking met de gemeente enkele preventieve maatregelen te treffen, zoals het bij snoeien van de groenvoorzieningen langs de paden, het aanbrengen van extra verlichting en het starten van een voorlichtingscampagne waarin werd aangegeven dat er preventieve maatregelen waren getroffen, zodat er geen reden meer was om zich onveilig te voelen. In de maanden die daarop volgden werden er echter meer mensen beroofd dan ooit. Het bleek dat de groep jonge overvallers die zich al enige tijd met name richtte op het park waar de fietsroutes doorheen liepen, zich niet liet weerhouden door de goede verlichting. Integendeel. Er keken toch geen huizen uit op het park en de overvallers vonden het wel prettig dat ze door de verlichting hun potentiële slachtoffers goed konden zien en ook of er andere mensen in de buurt waren. En ze verheugden zich ook over het feit dat het aantal alleenfietsende vrouwen de laatste tijd alleen maar toegenomen was.

1.2 Risico's

1.2.1 Risico-volle lokaties

Niet elk type onveiligheid komt op alle plekken in en rondom een zorginstelling even vaak voor. Preventie-inspanningen kunnen uiteraard het best gericht worden op de risico-lokaties en -situaties. Alhoewel deze per instelling ongetwijfeld variëren, kunnen wel enkele globale inschattingen worden gemaakt. Schema 1 geeft een overzicht.

Schema 1: Risico-lokaties binnen en buiten zorginstellingen

Risico-lokaties	Type onveiligheid
<i>Buiten</i>	
loop- en fietsroutes van en naar de instelling	exhibitionisme, aanranding, verkrachting, beroving
parkeerterrein	autodiefstal en inbraak auto
plekken waar (brom)fietsen worden gestald	(brom)fietsdiefstal, diefstal motoren
gebouwen/onroerende goeden op het terrein	vernieling en bekladding
de 'schil' van het gebouw	inbraak en brandstichting/spelen met vuur
<i>Binnen</i>	
lokaties waar veel klantencontact is (klantenbalie, SEH, verpleegafdeling, en dergelijke)	bedreiging en agressie
personeelsruimten	ongewenste intimiteiten
computernetwerk, administratie	fraude
overal waar veel waardevolle goederen zijn, die gemakkelijk meegenomen kunnen worden (onafgesloten kamers en opbergkasten van patiënten en personeel, garderobe, etc.)	diefstal

Dit schema biedt slechts een zeer globaal overzicht van risico-lokaties. Een meer nauwkeurige inschatting op maat kan per instelling worden gemaakt met behulp van het zogenaamde Ruimte-Risico-Inschattings Model (RRIM). Dit instrument is te vinden in bijlage 10. Andere instrumenten om risico-volle lokaties op het spoor te komen zijn de kleurenmethode (zie bijlage 3), die met name gericht is op onveiligheid van goederen en ruimten en de personeelsenquête (zie bijlage 4), die met name gericht is op (gevoelens van) onveiligheid van mensen.

1.2.2 Risico-vergrotenende factoren

Preventie richt zich op het, waar mogelijk, wegnemen van de factoren die onveiligheid veroorzaken. De volgende factoren zijn van invloed op de onveiligheidsproblemen van zorginstellingen:

- de locatie waar de instelling is gevestigd;
- de toegankelijkheid van de instelling;
- de aanwezigheid van voor criminelen aantrekkelijke objecten;
- de inrichting en aantrekkelijkheid van het gebouw en de omgeving;
- de grootte van de instelling;
- het soort mensen dat gebruik maakt van de instelling;
- de aanwezigheid van sociale controle en sociale netwerken;
- de kwaliteit van de arbeidsomstandigheden;
- de kwaliteit van de dienstverlening.

15

De locatie waar de instelling is gevestigd.

De aard en omvang van -met name de externe- criminaliteit en onveiligheidsgevoelens hangen samen met de urbanisatiegraad van de gemeente en kenmerken van de buurt waar de instelling is gevestigd. Een instelling is geen eiland, zodat het criminaliteitsniveau van de omgeving van invloed is op de onveiligheidsproblemen van de instelling. Ook de inrichting en het beheer van de openbare ruimte in de omgeving van de instelling zijn van invloed op de veiligheid in en rondom de instelling. Het verdient daarom aanbeveling om regelmatig overleg te voeren met de in dit kader van belang zijnde partners zoals de betrokken gemeentelijke diensten en afdelingen, de politie, andere (zorg)instellingen, bewonersplatformen e.d.

De toegankelijkheid van de instelling.

Hoe meer open de instelling van karakter is, des te groter zullen de onveiligheidsproblemen zijn. Met name diefstal binnen het gebouw zal dan een groot probleem zijn. De mate van openheid hangt sterk samen met het type instelling.

Algemene ziekenhuizen zijn het meest open in vergelijking met verzorgings- tehuizen en met name psychiatrische inrichtingen en zullen daarom relatief het meest last hebben van diefstal. Ziekenhuizen kiezen bovendien vaak uit het oogpunt van klantvriendelijkheid bewust voor een open karakter van hun instelling. Toch verdient het aanbeveling om kritisch te kijken naar b.v. het aantal ingangen wat de instelling kent.

Uit een security-audit bleek dat een bepaald ziekenhuis 120 in- en uitgangen had. Een voor de hand liggende beveiligingsmaatregel is dan: 110 uitgangen afsluiten.

Omdat een (open) gebouw in totaliteit lastig te beveiligen is, is het verstandig zich te richten op de toegankelijkheid van bepaalde risico-lokaties binnen het gebouw en die een extra hoge beveiligingsgraad te geven door middel van zonering en compartimentering.

De aanwezigheid van aantrekkelijke objecten

De inventaris van een algemeen ziekenhuis is in het algemeen zeer aantrekkelijk: bijna alles is bruikbaar. In andere typen zorginstellingen ligt het aantal aantrekkelijke objecten in het algemeen lager dan in ziekenhuizen.

Vlak voor de vakantie kennen de meeste ziekenhuizen een piek in het aantal diefstallen van bestek, servies, verbandmiddelen, medicijnen, scharen, spuiten, handschoenen, handdoeken etc. Naast deze gebruiksartikelen is ook medische apparatuur in trek. Deze apparatuur is veel geld waard en met name georganiseerde misdadigers lijken hier handel in te zien. Verder is een concentratie van (jonge) vrouwen (verpleeg-

sters), aantrekkelijk voor exhibitionisten, aanranders en verkrachters.

Persoonsgegevens dienen beschermd te worden in verband met mogelijke aantasting van de privacy. Een grote administratie en een uitgebreid computerbestand is tenslotte gevoelig voor fraude.

Zeer waardevolle goederen kunnen (indien mogelijk) het best in een afgesloten ruimte of kluis bewaard worden. Het aanstellen van toezichthouders of het anderszins bevorderen van de sociale controle is nuttig op plaatsen waar sprake is van een concentratie van goederen (parkeerplaatsen, stallingen, garderobes). Het met alarmvoorzieningen toerusten van personeel dat nachtdienst heeft en/of het zorgen dat verpleegsters 's nachts niet alleen het gebouw hoeven te verlaten, kan onveiligheidsgevoelens en het risico op seksuele delicten verminderen.

De inrichting en aantrekkelijkheid van het gebouw en de omgeving

De mate waarin gebruikers een band voelen met de instelling wordt beïnvloed door de aantrekkelijkheid van het gebouw en de omgeving. Zichtbare tekenen van criminaliteit, overlast en ander ongewenst gedrag verlagen de drempel om criminaliteit te plegen, terwijl tekenen die wijzen op de betrokkenheid van mensen bij het wel en wee van de instelling (verzorgde, aantrekkelijke omgeving, goed opgeruimd, schoongehouden en gezellig ingericht gebouw) de drempel juist hoger maakt. Bovendien voelen de gebruikers zich dan minder snel onveilig.

Ook de inrichting van het gebouw en de directe omgeving blijkt van invloed te zijn op de omvang van criminaliteit en onveiligheidsgevoelens. Zicht en overzicht is in dit verband belangrijk, wat bereikt kan worden met behulp van ruimtelijke ingrepen (door-dachte inrichting van balie-ruimten, heldere routing en bewegwijzering), goede verlichting en beheer (snoeien van groenvoorzieningen bijvoorbeeld).

Een uitgebreid overzicht van alle aspecten van de sociale en fysiek/ruimtelijke omgeving die van invloed zijn op de criminaliteit en onveiligheidsgevoelens is te vinden in het proefschrift 'Sociale veiligheid en gebouwde omgeving' van D.J.M. Van der Voordt en H.B.R. Van Wegen, dat is uitgegeven door de Faculteit der Bouwkunde van de Technische Universiteit Delft in 1991.

De grootte van de instelling.

Hoe meer gebouwen de instelling kent en hoe meer mensen gebruik maken van deze gebouwen, des te groter zullen de onveiligheidsproblemen zijn. Ook dit hangt samen met het type instelling. Aan deze factor is weinig te doen, behalve dat het beveiligingsniveau hierop afgestemd dient te worden.

Het soort mensen dat gebruik maakt van de instelling.

Het maakt uit of een instelling met name gebruikt wordt door 'vaste' klanten (vaste bewoners van een verzorgingstehuis of psychiatrische inrichting, familieleden die elke week oma komen bezoeken) of dat er sprake is van een komen en gaan van per dag verschillende bezoekers en patiënten, zoals in een ziekenhuis. Hoe groter en gevarieerder de gebruikersstroom, des te moeilijker is het om hier overzicht over te houden en om mensen die in de instelling niets te zoeken hebben te weren.

Het type mensen dat gebruik maakt van de instelling is ook heel bepalend voor het type problemen waar de instelling met name mee zal kampen. Zo zullen psychiatrische inrichting het meest met agressie en geweld van patiënten tegen personeelsleden kampen en zullen verzorgingstehuizen het meest alert moeten zijn op de onveiligheidsgevoelens van hun bewoners.

Instellingen dienen extra alert te zijn op onveiligheidsgevoelens bij de volgende risico-groepen:

- vrouwen, met name als ze 's avonds of 's nachts in en rondom de instelling moeten vertoeven (b.v. verpleegsters die nachtdienst hebben);
- personeelsleden die regelmatig te maken krijgen met agressieve klanten (SEH-ers, balie-medewerkers, personeel in psychiatrische inrichtingen e.d.);
- ouderen (voelen zich sneller onveilig);
- personeelsleden die al eens slachtoffer zijn geworden van een (seksueel) geweldsdelict op de werkplek.

Bij de voorlichting aan patiënten en personeel moet ervoor gewaakt worden om mogelijke onveiligheidsgevoelens bij deze risico-groepen niet te versterken. Ook kan gedacht worden aan het organiseren van fysieke en mentale weerbaarheidstrainingen voor bepaalde risico-groepen (b.v. SEH- en balie-personeel) en het zorgdragen van een goede opvang van slachtoffers. Ten aanzien van dit laatste aspect valt binnen zorginstellingen nog veel winst te behalen: het blijkt namelijk dat in de meeste zorginstellingen een opvangprocedure nog ontbreekt⁴.

17

De aanwezigheid van sociale controle en sociale netwerken.

Sociale controle kan mensen ervan weerhouden om delicten te plegen en heeft bovendien een positieve invloed op het gevoel van veiligheid.

In zorginstellingen kan het niveau van sociale controle verhoogd worden door het aanstellen van extra beveiligingsfunctionarissen. Vruuchtbaarder **dan het vergroten van het aantal formele toezichthouders** is echter om te trachten het preventie-bewustzijn van alle medewerkers in de instelling te vergroten.

De kwaliteit van de arbeidsomstandigheden

Het is een publiek geheim dat veel diefstallen in zorginstellingen gepleegd worden door het eigen personeel. Zo schat een veiligheidsfunctionaris van een ziekenhuis in Amsterdam dat minimaal 50% van de criminaliteit in het ziekenhuis veroorzaakt wordt door de eigen werknemers. Goede manieren om dit tegen te gaan is om te zorgen voor een goed personeelsbeleid, goede arbeidsomstandigheden en een prettig arbeidsklimaat. Als de instelling goed is voor z'n personeel, zal het personeel namelijk in het algemeen ook goed zijn voor de instelling. Hier wordt duidelijk dat beveiliging en arbo-zorg samenhangen. In hoofdstuk 2 zal hier nader bij stilgestaan worden.

De kwaliteit van de dienstverlening

Agressie in zorginstellingen ontstaat veelal als klanten vinden dat ze slecht behandeld worden. Ook diefstal en andere criminaliteit door patiënten en/of bezoekers wordt eerder gepleegd als men geen binding heeft met de instelling. Het zorgdragen voor een goede kwaliteit van de dienstverlening kan de band die klanten voelen met de instelling verbeteren en criminaliteit voorkomen. Kwaliteitszorg en beveiliging blijken dus samen te hangen. Ook dit zal in hoofdstuk 2 nader aan de orde komen.

⁴ Zie noten pagina 109

1.3 Gevolgen van onveiligheid

Materiële schade

De totale omvang van de materiële schade die zorginstellingen leiden als gevolg van criminaliteit, is onbekend. Voor ziekenhuizen variëren de schattingen van 8,5 miljoen (waarbij fijntjes opgemerkt wordt dat het ook best het twintigvoudige kan bedragen)⁵ tot 320 miljoen⁶ op jaarbasis. De grote verschillen tussen deze schattingen geven al aan dat de omvang van de schade zelfs niet bij benadering bekend is. Hoewel de totale schade-omvang onbekend is, blijkt wel uit onderzoek dat ruim 40% van de ziekenhuizen criminaliteit als een (redelijk) groot probleem beschouwt en dat 60% vindt dat de omvang van de problemen toeneemt⁷.

Immateriële schade

Naast direct in geld uit te drukken materiële schade ervaren met name slachtoffers agressie en (seksueel) geweld ook immateriële schade. Deze immateriële negatieve gevolgen van criminaliteit kunnen bestaan uit:

- verminderde prestaties op het werk, ziekteverzuim en arbeidsongeschiktheid
- verminderde uitoefening van de zorgplicht thuis, slechter verlopende sociale contacten met kinderen, partner, familie en vrienden
- verminderd plezier in vrijetijdsactiviteiten
- meer huisartsbezoek, meer gebruik van medicijnen
- toegenomen bezoek aan hulpverlenende instellingen

Uit onderzoek blijkt dat na een geweldsmisdrijf 16% van de medewerkers geen interesse meer hebben in het werk, 11% zich moeilijk kan concentreren, 48% bang is voor nieuw geweld, 11% problemen heeft in de relatie met de partner en 32% problemen heeft met psychisch functioneren (zich niet goed kunnen concentreren of snel wisselende stemmingen hebben).

Verslechtering van de arbeidsomstandigheden

Door agressieve en andere criminele incidenten raken medewerkers gedemotiveerd, men wordt onverschillig of cynisch. De collegialiteit gaat achteruit en de sfeer op de afdeling raakt verziekt, waardoor de kwaliteit van de werkplek aangetast wordt, met ongunstige gevolgen voor de arbeidssatisfactie en het ziekteverzuim. Behalve dat dit alles negatieve consequenties heeft voor de individuele medewerker, heeft het ook negatieve consequenties voor het ziekenhuis zelf. De negatieve gevolgen voor het ziekenhuis kunnen bestaan uit:

- verhoogd ziekteverzuim, met alle daaraan verbonden kosten (ziekteverzuimbegeleiding, de mogelijke malus etc.);
- mogelijke schadeclaims van werknemers vanwege inkomstenderving door een 'beroepsziekte';
- veel verloop onder het personeel, wat extra kosten veroorzaakt vanwege werving, selectie, opleiding en inwerken van nieuw personeel;
- verslechtering van het werkklimaat door afnemende motivatie en verminderde collegialiteit onder werknemers;
- prestatievermindering vanwege ontevredenheid met het werk.

Bovendien kan de omvang van de criminaliteit steeds verder gaan toenemen, omdat het personeel in een slecht arbeidsklimaat eerder zelf over zal gaan tot het plegen van diefstal e.d. Hierdoor kan de instelling in een opgaande criminaliteits-spiraal terecht komen.

Afnemende kwaliteit van de dienstverlening

Wanneer aan werknemers die slachtoffer zijn geworden van criminaliteit (met name van geweldsdelicten) geen hulp wordt geboden, kan dit op de lange duur ook negatieve gevolgen hebben voor de kwaliteit van de dienstverlening: wanneer men zelf geen aandacht en steun heeft gekregen is het moeilijk om dat wel voor anderen op te brengen. Maar ook de toenemende onveiligheidsgevoelens kunnen medewerkers demotiveren en de kwaliteit van de zorg doen verminderen.

Zorginstellingen zijn verantwoordelijk voor het welzijn van hun 'gasten'. Ook patiënten kunnen echter tijdens hun verblijf in de instelling slachtoffer van criminaliteit worden. Omdat zij al ziek of anderszins zorgbehoevend zijn en daardoor minder weerbaar, komt zoiets vaak extra hard aan. Hun onveiligheidsgevoelens kunnen daardoor toenemen, hetgeen hun genezingsproces niet ten goede zal komen. Ook op een andere manier kunnen patiënten gedupeerd raken door criminaliteit. Door diefstal van medicijnen en medische apparatuur kan de kwaliteit van de geleverde diensten achteruit gaan en dit kan in het ergste geval zelfs onverantwoorde gezondheidsrisico's tot gevolg hebben. Dit laatste zal niet alleen de patiënt schaden, maar ook de naam van het ziekenhuis.

2 De beveiliging

2.1 Het beveiligingsniveau van zorginstellingen: ideaal en werkelijkheid

Op dit moment blijken de meeste zorginstellingen nog in de zogenaamde 'bewakers-fase' te vertoeven: de aandacht voor beveiliging blijft grotendeels beperkt tot het installeren van technische beveiligingsmiddelen en het aanstellen van beveiligingsfunctionarissen. Het beveiligingsbeleid (voor zover er al sprake is van expliciet beleid) wordt voornamelijk door de beveiligingsfunctionarissen vastgesteld en uitgevoerd, min of meer los van de behoeften van de lijnmanagers en is met name gericht op fysieke bedreigingen van buitenaf. Voor veel zorginstellingen staat bedrijfsbeveiliging dan ook gelijk aan target-hardening en manbewaking.

Wel lijkt het bewustzijn dat de menselijke factor één van de belangrijkste beveiligingsmiddelen is, langzaam terrein te winnen. Men begint zich te realiseren dat niet alleen daarvoor opgeleide en aangestelde beveiligingsfunctionarissen een bijdrage kunnen leveren aan het algemene beveiligingsniveau van een organisatie, maar dat in principe alle werknemers hieraan kunnen bijdragen. Verder bestaat de indruk dat bij instellingen het bewustzijn aan het toenemen is, dat beveiliging goed moet aansluiten bij de bedrijfscultuur en bedrijfsprocessen.

Het doel van dit handboek is om zorginstellingen te helpen om hun beveiliging op een hoger plan te brengen. Anders gezegd: om instellingen van de bewakersfase te geleiden op de weg naar integrale beveiliging.

Op weg naar integrale beveiliging worden vijf ontwikkelingsstadia doorlopen. Schema 2 geeft hiervan een overzicht.

Aan de hand van schema 2 kan elke individuele zorginstelling nagaan in welk ontwikkelingsstadium hun beveiliging zich bevindt.

Waarschijnlijk ontdekken de meeste zorginstellingen dan dat hun beveiliging nog in één van de eerste ontwikkelingsstadia zit. Dit beveiligingsstadium zal echter steeds minder voldoen gezien de toenemende onveiligheidsproblemen in zorginstellingen en de nieuwe wettelijke arbo-eisen. Het dichten van de toenemende kloof tussen het bestaande beveiligingsniveau en het gewenste beveiligingsniveau is echter niet eenvoudig. Er zijn namelijk een aantal behoorlijke obstakels te overwinnen om een werkelijk geïntegreerde beveiliging te realiseren:

- er is kennis over en inzicht in abstracte, organisatorische principes vereist;
- er zijn vaak lastig op gang te brengen organisatorische veranderingen nodig;
- het management dient deze nieuwe beveiligingsfilosofie actief uit te dragen en te ondersteunen, wat gezien de lage prioriteit die door het management meestal aan beveiliging wordt toegekend, vaak niet het geval is.

Bij de huidige stand van zaken moet gesteld worden dat kennis, veranderingsbereidheid en (last but not least) het draagvlak in het algemeen bij het management ontbreken. Hier moet dus aan gewerkt worden.

Schema 2: Matrix ontwikkelstadia beveiliging

	Houding management	Status van beveiliging	Probleemaanpak
<i>Stadium 1: onbekendheid</i>	Beveiliging is bewaking en target hardening. Beveiliging is zaak van beveiligers.	Beveiliging is losse, uitvoerende eenheid.	Men gaat problemen te lijf als ze zich voordoen. Onvoldoende probleemdefiniëring.
<i>Stadium 2: ontwaken</i>	Men erkent dat er beveiligingslacunes zijn, maar is niet bereid er tijd/geld in te steken.	Beveiliging wordt versterkt, maar nadruk blijft op uitvoerende taken (bewaking) en target hardening.	Problemen worden iets gerichter aangepakt, maar naar lange-termijn oplossingen wordt niet gezocht.
<i>Stadium 3: doorbraak</i>	Men leert meer over veiligheidsproblemen en begint in te zien dat een andere aanpak van beveiliging nodig is.	Er ontstaat direct contact tussen beveiliging en management. Beveiliging komt in de portefeuille van één van de topmanagers.	Beveiliging wordt systematisch aangepakt. Problemen worden rationeel benaderd en opgelost.
<i>Stadium 4: wijsheid</i>	Men formuleert actief een beveiligingsbeleid. Men past waar nodig de bedrijfsvoering aan. Men zoekt naar raakpunten met andere zorggebieden.	Beveiliging is een stafaangelegenheid geworden. Beveiliging wordt betrokken bij andere zorggebieden (Arbo, milieu, kwaliteit).	Beveiligingsproblemen worden in een vroeg stadium gesignaleerd. Alle afdelingen/functies staan open voor verbeteringssuggesties.
<i>Stadium 5: zekerheid</i>	Men ziet beveiliging als een geïntegreerd onderdeel van de bedrijfsvoering en de bedrijfscultuur.	Een directielid is beveiligingsmanager. Beveiliging is een continu aandachtspunt geworden.	Beveiliging wordt geïntegreerd en pro-actief aangepakt. Bewaking/target hardening is sluitpost geworden.

In dit handboek zijn instrumenten en richtlijnen te vinden, die behulpzaam kunnen zijn bij het op een hoger plan brengen van beveiliging. Deze kennis en instrumenten zullen echter alleen optimaal toegepast worden, als het management overtuigd is van het belang van goede beveiliging. Deze overtuiging ontbreekt helaas nog al eens: beveiliging wordt vaak als een sluitpost beschouwd. Beveiliging wordt veelal uitbesteed aan een aparte beveiligingsafdeling en/of speciale beveiligingsfunctionarissen "die het verder maar moeten regelen". Deze beveiligingsfunctionarissen rapporteren meestal alleen aan het hoofd hoteldienst of het hoofd facilitair bedrijf, zodat de directie, het MT of de Raad van Bestuur vaak niet goed op de hoogte is van de zich voordoende problemen.

Om beveiliging op een hoger plan te krijgen is het essentieel dat beveiliging "in de lijn" wordt gebracht en een managementtaak wordt, die bij voorkeur verankerd wordt op directieniveau. En er zijn goede argumenten die pleiten voor meer bemoeienis van het management:

- 1 Goed georganiseerde beveiliging heeft een positief effect op de arbeidsomstandigheden en beschermt de kwaliteit van de dienstverlening en het imago van de instelling.
- 2 De integrale aanpak van agressie en (seksuele) intimidatie op de werkplek is sinds de invoering van de nieuwe Arbo-wet wettelijk verplicht. Indien werkgevers deze criminaliteitsrisico's verwaarlozen, kunnen tegen hen sancties worden ondernomen.
- 3 Goed georganiseerde beveiliging kan winst opleveren.
Niet alleen kan de (im)materiële schade van onveiligheid teruggedrongen worden, maar er kan bij een integrale beveiligingsaanpak ook gebruik gemaakt worden van de synergie-mogelijkheden die de overlappingen tussen kwaliteitszorg, arbo-zorg en beveiliging bieden. Hier zal in de volgende paragraaf nader op ingegaan worden.

2.2 Het verband tussen beveiliging, arbo-zorg en kwaliteitszorg: op zoek naar synergie

Als reactie op maatschappelijke ontwikkelingen en wettelijke eisen zijn bedrijven en instellingen in toenemende mate aandacht gaan besteden aan kwaliteits- en arbo-zorg. In het algemeen geldt dat arbo- en kwaliteitszorg in bedrijven en instellingen al aardig ver ontwikkeld zijn.

Recent en nog maar in beperkte kring is het bewustzijn ontstaan dat er opvallende overeenkomsten bestaan tussen kwaliteitszorg, arbo-zorg en milieuzorg. Wij willen de aandacht vestigen op het feit dat er ook opvallende overeenkomsten bestaan tussen kwaliteitszorg en arbo-zorg enerzijds en het 'zorggebied beveiliging' anderzijds. Sinds per 1 oktober 1994 de nieuwe arbo-wet is ingevoerd, zijn werkgevers verplicht gesteld om agressie, geweld en seksuele intimidatie jegens medewerkers te voorkomen en medewerkers die hier het slachtoffer van worden op te vangen⁸. Door deze uitbreiding van het arbo-zorggebied is er een duidelijke inhoudelijke overlap ontstaan tussen arbo-zorg en beveiliging.

Uitgebreide informatie over de gevolgen van deze wijziging van de arbo-wet is te vinden in de volgende publicatie:

Seksuele intimidatie, agressie en geweld; regels, feiten, aanpak, opvang

Praktijkreeks Arbo & Milieu, Samsom Bedrijfsinformatie, Alphen a/d Rijn/Zaventem, 1995

⁸ Zie noten pagina 109

Ook kwaliteitszorg kan overlappen met beveiliging. Zo vereist kwaliteitszorg een goed beheer van materialen, materieel en informatie binnen het bedrijf en aan een goed beheer zitten uiteraard security-aspecten zoals het tegengaan van onachtzaam gebruik, diefstal en vernieling.

Verder is de preventie en bestrijding van interne criminaliteit (een beveiligingstaak) van belang voor het realiseren van een kwalitatief goede bedrijfscultuur en werksfeer. Naast inhoudelijke overlappingsen bestaan er ook organisatorische overeenkomsten tussen de zorggebieden. Als een instelling bijvoorbeeld organisatie-veranderingen door wil voeren in het kader van een integraal kwaliteitsproject of als reactie op de veranderde eisen van de arbo-wet, liggen daar voor beveiliging ook veranderingskansen.

Een nadere uitwerking van deze geïntegreerde visie op beveiliging, waarbij op zoek gegaan wordt naar de synergie-mogelijkheden die de overeenkomsten tussen beveiliging, arbo- en kwaliteitszorg bieden, is te vinden in de publikatie:

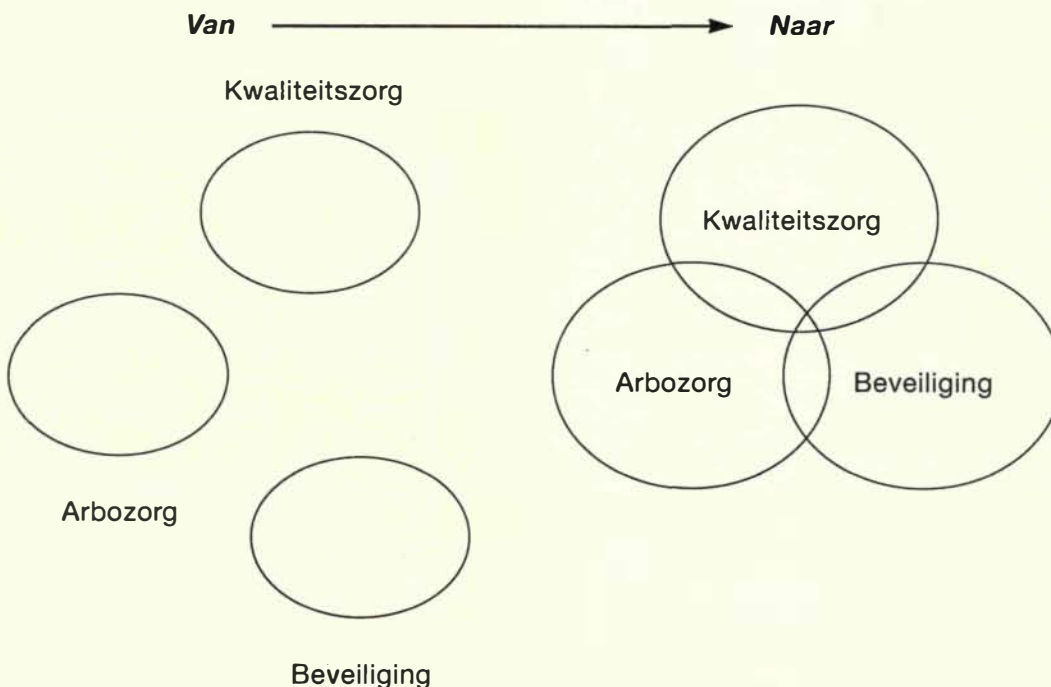
Beveiliging en bedrijfsvoering: naar een geïntegreerde aanpak

Van Dijk, Van Soomeren en Partners

Amsterdam 1994.

Door nu gebruik te maken van de overeenkomsten tussen de zorggebieden kan efficiënter en effectiever omgegaan worden met de aanwezige kennis en kostbare tijd en middelen, zodat er sprake is van 'synergie'. Dit kan zowel de veiligheidszorg ten goede komen als de andere twee zorggebieden⁹ en aldus het bedrijf in totaliteit.

Schema 3: Bewustwording van de samenhangen van zorggebieden



⁹ Zie noten pagina 109

Een vruchtbare strategie om beveiliging verder te ontwikkelen en winst voor het hele bedrijf te boeken luidt als volgt.

- 1 Wordt bewust van de overeenkomsten tussen de zorggebieden.
- 2 Ga vervolgens op zoek naar synergie-mogelijkheden: op welke manier kan in uw instelling beveiliging profiteren van de ontwikkelingen op het gebied van de kwaliteitszorg en arbo-zorg en vice versa?

Essentiële voorwaarde hierbij is wel dat men elkaars taal moet (leren) spreken: er kan alleen geprofiteerd worden van synergetische effecten als beveiligers weten wat kwaliteitsmanagers en Arbo-coördinatoren bezig houdt en vice versa.

Op dit moment zijn kwaliteitsmanagers en Arbo-coördinatoren over het algemeen niet geïnteresseerd in beveiliging en zij zullen ook niet snel hun best doen om de communicatie met de beveiligers te verbeteren. Ze zien daar niet het belang van in. Omdat beveiligers waarschijnlijk meer kunnen leren van de kwaliteits- en Arbo-deskundigen dan omgekeerd, zullen primair de beveiligers belang hebben bij een betere onderlinge communicatie en dienen zij daar in eerste instantie het meest in te investeren. Het is echter zeer wel denkbaar dat door de verbeterde communicatie de kwaliteits- en Arbo-deskundigen zich bewust worden van het belang van beveiliging, ook voor hun eigen zorggebied, zodat ze wellicht steeds meer bereid zijn om te investeren in een goede communicatie en uitwisseling van kennis en ervaring.

Beveiligers zouden, kortom, een **marketingbeleid** moeten ontwikkelen dat gericht is op het Arbo-zorggebied en het kwaliteitszorggebied: welke kennis heb ik als beveiligers waar de Arbo-zorg of de kwaliteitszorg iets aan heeft en op welke manier dien ik die kennis te verpakken opdat dat zorggebied geïnteresseerd raakt in mijn 'produkt' en dit af gaat nemen?

Twee concrete producten die beveiligers aan de andere zorggebieden te bieden hebben (maar die wel in een iets ander jasje gestoken zullen moeten worden), zijn de risico-analyse en de audit-systematiek. Wij komen hier later op terug.

2.3 Conclusies

De noodzaak voor integrale beveiliging van zorginstellingen neemt toe. Enerzijds omdat werkgevers sinds kort wettelijk verplicht zijn gesteld om minimaal een deel van de onveiligheid (agressie en geweld op de werkplek) integraal aan te pakken, anderzijds omdat het bewustzijn groeit dat onveiligheid veel schade en persoonlijk leed veroorzaakt bij mensen die belangrijk voor de instelling zijn (klanten en werknemers). Het verbeteren van beveiliging zal echter -zeker in het begin- aardig wat moeite kosten en een basisvoorwaarde vormt dan ook dat er genoeg draagvlak voor is bij het management. Het dient daarom bewust te worden gemaakt van het feit dat integrale beveiliging ten goede kan komen aan de kwaliteit van de arbeidsomstandigheden en de dienstverlening, zaken die het management van een zorginstelling aan het hart gaan. Verder zal een goede beveiliging op termijn de inzet van mensen en middelen effectiever kunnen maken en de instelling geld kunnen besparen.

Indien de wil bij het management er is **en beveiliging hoger op de agenda wordt geplaatst**, kan dit handboek in de praktijk goede diensten bewijzen. Het handboek geeft namelijk de kennis en de instrumenten om beveiliging op een hoger plan te brengen en uiteindelijk het pad op te slaan richting integrale beveiliging.

Deel II De weg naar de integrale beveiliging

25

3 Het preventiewiel

Stel u bent verantwoordelijk voor de beveiliging van uw instelling en u krijgt steeds vaker te maken met criminele voorvallen. Hoe kunt u die onveiligheidsproblemen nu het beste aanpakken? Ons uitgangspunt is dat een integrale benadering van het beveiligingsvraagstuk hiervoor de beste manier is. Zoals in het vorige hoofdstuk aangegeven, bedoelen we daarmee dat veiligheidszorg afgestemd dient te zijn op Arbozorg en kwaliteitszorg.

Er zijn echter pas goede garanties voor de beveiliging van uw instelling wanneer een systeem van integrale beveiliging gerealiseerd wordt. Met "integraal beveiligingssysteem" doelen we op een systeem waarin voortdurend aandacht wordt geschonken aan vier elementen, namelijk

- het beveiligings*beleid*
- de beveiligings*organisatie*
- de beveiligings*voorzieningen*
- de beveiligings*cultuur*.

Door de aandacht te spreiden over deze aspecten wordt de beveiligingsproblematiek in de volle breedte bekeken en wordt voorkomen dat te snel gezocht wordt naar ad hoc oplossingen voor deelproblemen.

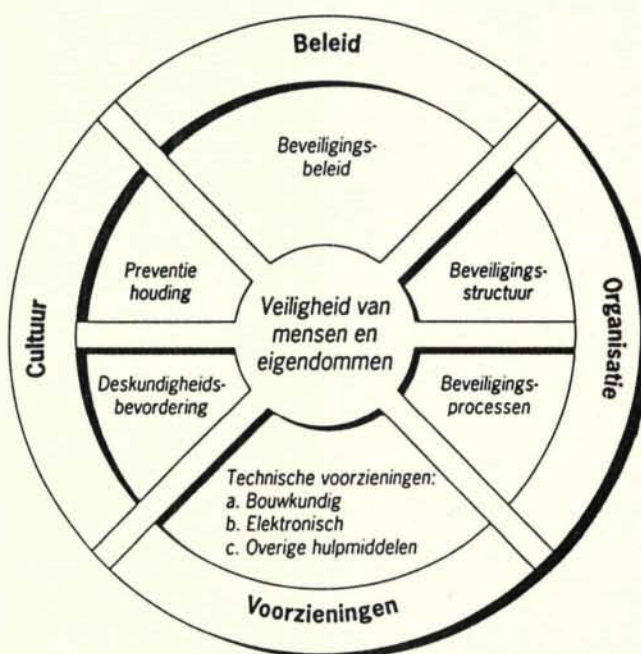
Het tot stand brengen van een beveiligingssysteem waarin aan die vier factoren binnen de instelling aandacht wordt geschonken, is een taak van security-management.

DamhuisElshoutVerschure heeft een instrument ontwikkeld waarin de bovengenoemde aspecten zijn verwerkt. Dit instrument wordt het **Preventiewiel** genoemd.

Het Preventiewiel is een hulpmiddel bij het realiseren van een integraal beveiligingssysteem. Met behulp van het Preventiewiel worden die factoren in beeld gebracht die noodzakelijk zijn om objectieve en subjectieve veiligheid van mensen en eigendommen te realiseren. Op basis daarvan wordt de diagnose van de bestaande beveiligingssituatie van een organisatie vastgesteld. Met de diagnose biedt het Preventiewiel tegelijkertijd ook de aanknopingspunten voor de te nemen maatregelen en middelen. In schema 4 staat het Preventiewiel afgebeeld.

Schema 4: Het preventiewiel

26



In de volgende paragrafen geven we een beschrijving van de elementen* van een integraal beveiligingssysteem dus van het het Preventiewiel.

* Bij elk element horen vragen die voor het inventariseren van de bestaande beveiligingssituatie van belang zijn. Door de vragen te beantwoorden komt men op ideeën en randvoorwaarden die belangrijk zijn voor het concrete vraagstuk van beveiliging. In bijlage 5 zijn deze vragen opgenomen. Deze vragen worden ook gehanteerd bij de in paragraaf 4.3.4 beschreven security-audit.

3.1 Het beveiligingsbeleid

Het beveiligingsbeleid is het onder verantwoordelijkheid van het management ontwikkelde beleid van een organisatie ten aanzien van beveiliging. Dit beleid dient gebaseerd te zijn op de resultaten van een intern veiligheidsonderzoek en beschreven in een beveiligingsbeleidsplan. Dit plan bevat tevens de visie van de organisatie op beveiliging. Deze visie wordt bepaald door het karakter van een instelling. Een open organisatie met frequente grote stromen bezoekers zal een andere visie op beveiliging dienen te ontwikkelen dan een gesloten instelling met weinig bezoekers. In het beveiligingsbeleidsplan worden tevens de maatregelen en middelen beschreven die gericht zijn op het realiseren van objectieve en subjectieve veiligheid. Het plan kan maatregelen voor de korte, middellange en lange termijn bevatten. Daarnaast dient ook de samenhang met de Arbozorg en de kwaliteitszorg aangegeven te worden. In zekere zin vormt het beleidsplan het startpunt en het sluitstuk van een project waarin met behulp van het Preventiewiel een analyse van de beveiligingssituatie gemaakt is. In paragraaf 4.4.2 gaan wij in op de inhoud van een beveiligingsbeleidsplan.

27

3.2 De Beveiligingsorganisatie

De organisatie van de beveiliging bestaat uit een beveiligingsstructuur en de beveiligingsprocessen die plaatsvinden.

3.2.1 De beveiligingsstructuur

In de organisatiestructuur van een instelling dient de aandacht voor beveiliging verankerd te zijn. Van een beveiligingsstructuur is sprake wanneer

- . binnen de organisatie functionarissen met duidelijk omschreven taken en verantwoordelijkheden zijn aangesteld voor de beveiligingstaak
- . hun positie in de organisatie voor iedereen duidelijk is en geaccepteerd wordt
- . een herkenbare lijn loopt vanaf de voor beveiliging verantwoordelijke directeur, via de verantwoordelijke leidinggevenden naar de uitvoerende medewerkers
- . duidelijk is wat van andere leidinggevenden en collega-medewerkers verwacht wordt ten aanzien van beveiliging (horizontale afstemming).

Voor de goede orde maken wij u attent op het volgende. Wanneer onderdelen van de organisatie formeel (mede) belast worden met de feitelijke handhaving van de veiligheid van personen en goederen of van de openbare orde en rust, worden deze onderdelen ingevolge de Wet op de Weerkorpsen en de Particuliere Beveiligingsorganisaties aangeduid als particuliere beveiligingsorganisaties. Bijgevolg dienen deze onderdelen te voldoen aan de daaraan in de betreffende wet gestelde eisen. De Wet op de Weerkorpsen wordt op dit moment overigens herzien.

3.2.2 De beveiligingsprocessen

Beveiligingsprocessen zijn het geheel van beschreven en vaste organisatorische regelingen. Goed doordachte procedures en voorschriften die bij iedereen bekend zijn en waarop controle bestaat, zijn voor een goed beveiligingsbeleid onmisbaar. Zij zijn nodig om de beveiligingsorganisatie soepel te laten lopen en voorkomen dat er vaak overleg en improvisatie dient plaats te vinden in situaties waar snel en effectief optreden vereist is.

We denken hierbij aan regelingen met betrekking tot

- . toegangsbeheer
- . opvang van personen die binnen de instelling slachtoffer zijn geworden van een vorm van criminaliteit

- melding van incidenten
- databeheer
- de opslag van privacy-gevoelige patient- en persoonsgegevens
- alarmering
- voorraadbeheer
- calamiteiten
- controle en inspectie
- afspraken met politie
- taken en bevoegdheden beveiligingspersoneel

Onder wordt een korte beschrijving van deze regelingen gegeven.

Toegangsbeheer

Een regeling toegangsbeheer omvat het geheel van procedures en richtlijnen waarmee de organisatie de toegang door fysieke barrières regelt en controleert; hieronder vallen onder meer de uitgifte en het beheer van sleutels. Daarnaast is het ook van belang een autorisatie-overzicht op te stellen. Door het toepassen van effectieve procedures en richtlijnen alsmede de waakzaamheid van medewerkers, kan de organisatie personen identificeren, die wel of geen toegang hebben tot het gebouw, afdelingen of bepaalde ruimten daarin.

Opvang van personen die binnen de instelling slachtoffer zijn geworden van criminaliteit

De opvang en begeleiding van personen, die binnen de instelling slachtoffer zijn geworden van criminaliteit, bij de verwerking van de gevolgen van gewelddadige incidenten die binnen de instelling hebben plaatsgevonden dient in procedures en richtlijnen geregeld te zijn.

Melding van incidenten

Ten behoeve van het beveiligingsbeleid is het van belang te kunnen beschikken over een accurate databank wat betreft oorzaak en aard van incidenten die zich in en rondom de organisatie voordoen. Een procedure voor melding incidenten is dan ook noodzakelijk. In deze procedure dient aangegeven te worden op welke wijze incidenten dienen te worden gerapporteerd, vastgelegd, afgehandeld en geanalyseerd.

Databeheer

In een regeling databeheer worden de procedures en richtlijnen beschreven waarmee de beveiliging van de toegang tot computer(s), de programma's en de bestanden wordt geregeld.

De opslag van privacy-gevoelige patiënt- en persoonsgegevens

In deze regeling zijn de procedures en richtlijnen vastgelegd met betrekking tot het verzamelen, verwerken, distribueren en beveiligen van privacy-gevoelige gegevens.

Alarmering

In een regeling alarmering wordt een actieplan beschreven alsmede de procedures en instructies die alle betrokkenen dienen te volgen in geval van (agressieve) incidenten.

Vorraadbeheer

Een regeling voorraadbeheer beschrijft de procedures en richtlijnen voor een helder registratie-en controlesysteem ten behoeve van alle fasen van het proces van ontvangen en distribueren van goederen binnen de organisatie.

Een calamiteitenplan

In een calamiteitenplan staan alle noodzakelijke handelingen beschreven die uitgevoerd dienen te worden in noodsituaties en die tot doel hebben:

- levens van mensen te redden en het aantal gewonden te beperken
- eigendommen te beschermen tegen beschadiging
- dat de organisatie haar essentiële functies kan blijven uitvoeren.

29

Controle en inspectie

In een regeling controle en inspectie dienen onder andere de afspraken beschreven te worden met betrekking tot het dienstrooster, het surveilleren in en rond het gebouw, het nalopen van deuren, ramen, verlichting en de rapportage daarvan door bewakingspersoneel.

Regeling afspraken met politie

In het kader van een beveiligingsbeleid is het gewenst dat op instellingsniveau goede werksafspraken met de politie gemaakt zijn.

Taken en bevoegdheden beveiligingspersoneel

De werkzaamheden kunnen inhouden:

- zelf bewakingstaken uitvoeren (surveilleren in en rond het gebouw, controleren van deuren, ramen, verlichting)
- signaleren van brand- en veiligheidsrisico's en hierop actie ondernemen intern (verantwoordelijke functionarissen) en extern (politie en dergelijke)
- registratie van voorvallen en rapportage (formuleren van voorstellen).

Het is van belang om in de functie-omschrijving, naast deze taken, ook vast te leggen:

- de plaats in de organisatie (verantwoording verschuldigd aan)
- de vaste overlegverbanden waarin de functionaris deelneemt
- het doel van de functie (bijdrage aan bestrijding van criminaliteit en verhogen van veiligheidsgevoelens)
- de bevoegdheden (controle- en signaleringsbevoegdheid en dergelijke).

3.3 Technische voorzieningen

Instellingen die gevraagd worden naar de maatregelen die zij getroffen hebben om mensen en eigendommen te beveiligen, presenteren meestal de technische en met name de elektronische voorzieningen als hun 'paradepaardjes'. Deze voorzieningen zijn echter alleen effectief als zij ingebed zijn in een adequaat beleid en in een efficiënt en effectief werkende structuur.

Onderscheiden worden bij technische voorzieningen

- . bouwkundige voorzieningen
- . elektronische voorzieningen
- . overige hulpmiddelen

Bouwkundige voorzieningen betreffen fysieke maatregelen die getroffen worden om criminaliteitsrisico's zo klein mogelijk te maken. Bouwkundige voorzieningen worden doorgaans te laat getroffen, namelijk als de bouw al gerealiseerd is. In principe moeten bouwkundige maatregelen in verband met beveiligingseisen reeds in het Programma van Eisen opgenomen worden. Het gaat bijvoorbeeld om voorzieningen die het aantal onbewaakte in- en uitgangen beperken en het voorkomen van ruimten die buiten de sociale controle vallen.

Bij elektronische voorzieningen moet gedacht worden aan voorzieningen als een gesloten tv-circuit, communicatiesystemen (alarm, draadloze telefoon, piepers), inbraakdetectie van ruimten en op deuren (met een meldcentrale), een elektronisch slotensysteem en een toegangscontrolesysteem.

In de restcategorie overige vallen voorzieningen die meer zijn dan puur organisatorische maatregelen en derhalve investeringskosten met zich meebrengen. Hierbij kan gedacht worden aan een badgesysteem.

3.4 Cultuur

Een goede beveiligingscultuur is te zien als de drager van een beveiligingssysteem en wordt gerealiseerd door deskundigheidsbevordering en via een goede preventiehouding bij het personeel. Een goede beveiligingscultuur blijkt onder andere uit:

- . de discipline waarmee de medewerkers binnen een organisatie de beveiligingsvoorschriften naleven
- . de (sociale) controle op de naleving van de beveiligingsvoorschriften
- . de alertheid waarmee de organisatie op incidenten reageert

3.4.1 Deskundigheidsbevordering

Door middel van opleidingen, cursussen, thema-dagen, trainingen en het verspreiden van schriftelijk materiaal kan de deskundigheid van mensen binnen de instelling bevorderd worden.

In z'n algemeenheid dient het informatieniveau en de alertheid op peil gehouden te worden door informatie- en instructiebijeenkomsten over risico's, voorvallen en gedragsregels.

Deskundigheidsbevordering kan zich op de volgende doelgroepen richten:

- . De specialistische beveiligingsfunctionarissen op beleids- en uitvoeringsniveau.
Zij dienen te voldoen aan de deskundigheidseisen en specifieke opleidingen op dit terrein te volgen.
- . De medewerkers in de organisatie.
Zij dienen vanaf hun binnenkomst (stage, opleidings- en introductieperiode) goed geïnstrueerd te worden over de beveiligingsmaatregelen en daarbij horende activiteiten.
- . De patiënten/cliënten.
Zij dienen voorgelicht te worden over de door hen zelf te nemen maatregelen en de door de instelling getroffen maatregelen.

Inhoudelijk kan deskundigheidsbevordering zich op de volgende onderwerpen richten:

- Vakinhoudelijke kennis (b.v. bij specialistische beveiligingsfunctionarissen).
- Kennis over beveiligingsmaatregelen en procedures.
- Kennis over opvangmogelijkheden en procedures
- Het aanleren van vaardigheden (b.v. het leren omgaan met agressie).

In bijlage 9 wordt nader inhoudelijk ingegaan op mogelijkheden van deskundigheidsbevordering op het gebied van agressie en geweld.

3.4.2 Een preventiehouding

De houding van management en medewerkers vormt zowel het sluitstuk (resultaat) als het begin (de 'drager') van een goed beveiligingssysteem. Het gaat hier over de moeilijk grijpbare cultuurkant van een preventiesysteem. Het gaat om waarden en normen (wat hoort hier, wat mag wel of niet), om ingesleten gedragingen en om voorbeeldgedrag van kernfiguren in de organisatie.

De aanwezigheid van een goede preventiehouding blijkt vooral uit de mate waarin alle medewerkers in de organisatie zich medeverantwoordelijk voelen voor de beveiliging van eigendommen van de organisatie, van collega's, van patiënten/cliënten en van zichzelf.

4 Het ontwikkelen van een beveiligingssysteem in een zorginstelling

4.1 Fasen in het opzetten van een beveiligingssysteem

Bij het opzetten van een beveiligingssysteem dienen de volgende fasen doorlopen te worden.

De voorbereidende fase

In de eerste voorbereidende fase worden stappen ondernomen die leiden tot:

- 1 een draagvlak voor het houden van een project integrale beveiliging
- 2 het opzetten van een projectorganisatie beveiliging
- 3 het maken van een projectplan van aanpak
- 4 de formele vaststelling van het plan van aanpak.

De analyse-fase

In deze tweede fase worden de onderzoeksinstrumenten toegepast die gegevens opleveren over de huidige beveiligingssituatie van de instelling. De resultaten van het onderzoek vormen de basis voor het op te stellen beveiligingsbeleidsplan. De resultaten kunnen tevens dienen als voormeting voor een later te houden effect-evaluatie.

De beleidsfase

In deze derde fase worden de onderzoeksgegevens verwerkt en het beveiligingsbeleidsplan geschreven.

De uitvoerings- en evaluatiefase

In de vierde fase worden de aanbevelingen van het beveiligingsbeleidsplan uitgevoerd en na enige tijd geëvalueerd. Na verloop van tijd zal de beveiliging meer en meer betrokken worden bij andere zorggebieden zoals de Arbo en kwaliteit. Geleidelijk wordt de beveiliging een geïntegreerd onderdeel van de bedrijfsvoering en de bedrijfscultuur. Beveiliging is een continu punt van aandacht binnen de instelling geworden. De doelstellingen met betrekking tot beveiliging worden in een vast patroon geëvalueerd en waar nodig worden uitgangspunten en doelstellingen bijgesteld.

De fasen zullen in dit hoofdstuk één voor één uitgewerkt worden.

Deze benadering is in eerste instantie uitgeprobeerd in het Flevo Ziekenhuis in Almere en verder toegepast in de projecten "Sociale Veiligheid in en rond zorginstellingen te Flevoland" en "Sociale Veiligheid, ons een zorg!" in Twente en Utrecht. In Twente heeft een evaluatie-onderzoek plaatsgevonden waarvan de resultaten in deze handleiding zijn verwerkt.

4.2 De voorbereidende fase

4.2.1 Het verkrijgen van draagvlak

Een project integrale beveiliging heeft alleen kans van slagen als daarvoor voldoende draagvlak bestaat bij **iedereen** binnen de organisatie. Draagvlak ontstaat wanneer alle betrokkenen in de organisatie een voldoende besef hebben van de beveiligingsproblemen en het nut en de noodzaak van een aanpak daarvan zien. In deze eerste fase dient met name bij de directie, de ondernemingsraad en collega's van het management-team draagvlak ontwikkeld te worden.

Realiseert u zich goed dat draagvlak niet van de ene op de andere dag ontstaat. Het motiveren van mensen is een kwestie van lange adem hebben. Tijdens het project zal aan dit aspect steeds aandacht besteed dienen te worden. Het geven van informatie is daarbij het belangrijkste middel dat u ter beschikking staat. In deze handleiding geven wij de momenten aan waarop u kunt werken aan verhoging van het draagvlak binnen de organisatie.

33

Op welke wijze kan het management overtuigd worden?

1 Geef informatie over de problematiek¹⁰

- Geef inzicht in de (geschatte) omvang en schade van onveiligheid en wijs op de emotionele gevolgen van onveiligheid voor klanten en personeel.
 - Geef aan hoe onveiligheid de kwaliteit van de werkplek aantast.
 - Laat zien hoe onveiligheid de kwaliteit van de dienstverlening beïnvloedt.
 - Wijs op de wettelijke noodzaak om onveiligheid (althans een belangrijk deel daarvan, namelijk agressie en geweld) aan te pakken.
 - Vestig de aandacht op de externe publiciteit over de problematiek en wijs op het gevaar van negatieve publiciteit.
- U kunt hierbij gebruik maken van artikelen uit de Knipselkrant van het Nationaal Ziekenhuis Instituut.

2 Wijs op de noodzaak van een gedegen aanpak

Geef aan dat de beveiligingsproblematiek goed aangepakt dient te worden en dat een integrale aanpak daartoe de beste weg is. Leg uit wat de opzet van een integraal beveiligingssysteem inhoudt en laat de voordelen ervan zien. Wijs op het gevaar van ad hoc oplossingen: lapmiddelen met veelal een beperkt rendement.

Leg ook uit dat een projectmatige aanpak van de problematiek gewenst is. Met een projectmatige aanpak wordt binnen een bepaalde periode en met beperkte middelen naar een concreet omschreven doel gewerkt, waarbij meerdere disciplines en onderdelen van de organisatie worden ingezet. Dit draagt bij aan de verhoging van het draagvlak voor beveiliging binnen de instelling.

3 Zoek samenwerking met instellingen uit de regio

Andere instellingen in uw regio hebben vaak te maken met dezelfde beveiligingsproblemen. Het is om meerdere redenen zinvol de beveiligingsproblematiek samen met collega-instellingen aan te pakken. Dit was het geval bij de projecten "Veiligheid ons een zorg!" van de Twentse en Utrechtse ziekenhuizen en "Sociale Veiligheid in en rond zorginstellingen in Flevoland". Naast de bundeling van aanwezige kennis en deskundigheid (onder andere over de toepassing van technieken, aanschaf van beveiligingsvoorzieningen en deskundigheidsbevordering) kunnen de instellingen gezamenlijk ins-

¹⁰ Zie noten pagina 109

trumenten als bijvoorbeeld voorlichtingsmateriaal, enquêteformulieren, protocollen en dergelijke ontwikkelen. Zij kunnen elkaar verder behulpzaam zijn bij bepaalde werkzaamheden (voorlichting, training en scholing van medewerkers en uitvoeren van security-audits) en bij het beoordelen van plannen en adviseren over mogelijk te ondernemen stappen. Ook zijn er financiële voordelen verbonden aan het gezamenlijk ondernemen van maatregelen en activiteiten bijvoorbeeld ten aanzien van de gezamenlijke aanschaf van beveiligingsvoorzieningen en het inhuren van toezicht/beveiliging. Een gemeenschappelijke aanpak blijkt in de praktijk tevens een motiverende factor te hebben. Een instelling kan immers moeilijk als enige afhaken. Daarmee zou de schijn gewekt kunnen worden als zou de instelling geen of onvoldoende waarde hechten aan het beveiligingsvraagstuk.

Zoek ook samenwerking met de regiopolitie. Deze vervulde in alle hiervoor genoemde projecten een belangrijke rol door haar deskundigheid en ervaring op het terrein van beveiliging. Ook met het oog op nog nader te maken samenwerkingsafspraken met de regiopolitie, is dit van belang.

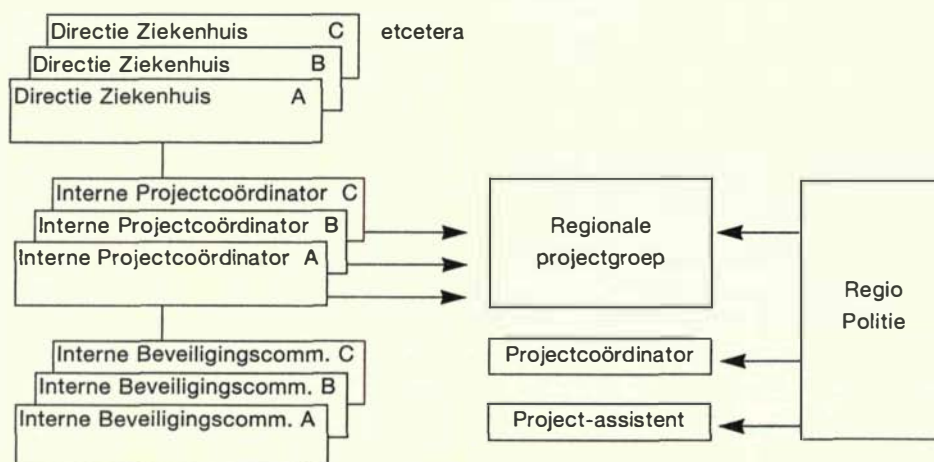
Bekrachtig de samenwerking met uw collega-instellingen wel met een overeenkomst die op directieniveau door alle belanghebbenden wordt ondertekend. In een samenwerkingsovereenkomst of samenwerkingsconvenant worden een aantal zaken en verplichtingen nog eens duidelijk vastgelegd. Een samenwerkingsovereenkomst vormt tevens de opdracht voor een in te stellen regionale projectgroep. In bijlage 6 is een voorbeeld van een samenwerkingsconvenant opgenomen.

Bij het ziekenhuisproject 'Veiligheid ons een zorg!' in Twente en Utrecht, had de afsluiting van de overeenkomst door directies van betrokken ziekenhuizen en andere deelnemers ook een andere belangrijke functie. Het betekende een duidelijke markering van het officiële begin van het project. Door het officiële startschot door de directies te laten maken, legden de organisaties zichzelf min of meer vast en voelden ze zich verbonden om het project samen tot een goed einde te brengen.

4.2.2 Het opzetten van een projectorganisatie beveiliging

In deze handleiding gaan wij uit van een samenwerking tussen meerdere instellingen die bekrachtigd is met een samenwerkingsconvenant en het instellen van een regionale stuurgroep.

Onder is de projectorganisatie van de ziekenhuisprojecten in Twente, Utrecht en Flevoland tijdens de ontwikkelingsfase schematisch weergegeven:



De regionale projectgroep

De ziekenhuisprojecten in Twente en Utrecht hadden een regionale projectgroep die tijdens de startfase van het project een belangrijke rol vervulde. Een dergelijke projectgroep bestond ook in Flevoland.

De regionale projectgroep bestond naast de projectcoördinator en project-assistent uit de interne projectcoördinatoren van de instellingen.

Taken van een regionale projectgroep waren:

- de centrale regievoering van de beveiligingsprojecten in de instellingen
- gezamenlijk ontwikkelen van instrumenten, zoals bijvoorbeeld
 - . voorlichtingsmateriaal
 - . enqueteformulieren
 - . aangifte-/incidentenformulieren
 - . protocollen etcetera
- gezamenlijk opzetten en uitvoeren van beveiligingsactiviteiten, zoals bijvoorbeeld
 - . het geven van voorlichting
 - . uitvoering van security-audits
- het bieden van een kader voor overleg en uitwisseling van ervaringen tussen interne projectcoördinatoren
- platform voor kwaliteitsbewaking en deskundigheidsbevordering
- het beoordelen van plannen en het geven van adviezen over mogelijk te ondernemen stappen.

35

Na beëindiging van het project kan de regionale projectgroep, zonder de projectcoördinator en project-assistent, een vast organisatorisch verband van de instellingen worden. Zo'n verband kan diverse vormen hebben:

- een periodiek overleg
- een samenwerkingsverband van waaruit gezamenlijke afspraken gemaakt worden. Te denken valt aan het afsluiten van overeenkomsten met particuliere beveiligingsorganisaties bijvoorbeeld over detachering van beveiligingspersoneel of de gemeenschappelijke inkoop van beveiligingsmiddelen
- een vorm waarbinnen uitwisseling van aanwezige capaciteiten kan plaatsvinden
- een gezamenlijke beveiligingsorganisatie.

De doelstelling om voor de instelling heldere, werkzame beveiligingsorganisatie op te zetten, veronderstelt dat de lijnverantwoordelijkheid is geregeld en dat er op uitvoerend niveau functionarissen beschikbaar zijn.

De projectcoördinator

De projectcoördinator vormt een belangrijke spil in het project. Hij/zij vormt samen het centrale coördinatie- en aanspreekpunt. In de projecten is gebleken dat de functie essentieel is voor de voortgang van het proces. Wanneer voor deze functie niet een aantal uren wordt vrijgemaakt, ontbeert het proces de 'motor'. Dan bestaat het gevaar van een tijd- en energierovend proces dat weinig concreet rendement opleverd. Middelen voor een dergelijke projectondersteuning zijn met andere woorden een randvoorwaarde voor een goed beveiligingsproject.

Taken van een projectcoördinator zijn:

- geeft leiding aan het project
- draagt zorg voor de afstemming en bewaking van de uit te voeren beveiligingsactiviteiten
- rapporteert, overlegt en draag zorg voor afstemming met de directies van de betrokken instellingen

- is voorzitter van de regionale projectgroep
- beheert het projectbudget
- treedt op als contactpersoon naar de politie.

Voorwaarden voor functioneren projectcoördinator en regionale projectgroep:

- duidelijkheid over taken, verantwoordelijkheden en bevoegdheden
- het beschikken over een gegarandeerd minimum aan tijd ten behoeve van de projectcoördinatie
- de regionale projectgroep bestaat uit vaste leden die een behoorlijk deel van hun werktijd voor de uit het project voortvloeiende beveiligingsactiviteiten beschikbaar hebben
- het hebben van toegang tot en mogelijkheden voor het verzamelen, vastleggen, bewaren, verwerken, vermenigvuldigen, distribueren en presenteren van gegevens die van belang zijn voor het project
- de beschikking over een eigen projectbudget
- ondersteuning van een project-assistent.

36

Hiertoe zullen doelstellingen, plannen, budgetten, spelregels, procedures en dergelijke met alle deelnemende instellingen duidelijk dienen te worden overeengekomen en vastgelegd.

De project-assistent

De project-assistent vormt een onmisbare schakel in het gehele project. De project-assistent ondersteunt de projectcoördinator bij diens taken en draagt in belangrijke mate bij tot de continuïteit van het project.

Taken project-assistent

- secretariële ondersteuning van het projectbureau
- notuleren van de regionale projectgroepvergaderingen
- bewaken van de planning
- ondersteuning geven bij verwerking en rapportage onderzoeksresultaten.

De interne beveiligingscommissie

Om draagvlak voor de beveiliging binnen de instelling te realiseren dient een zo breed mogelijk samengestelde beveiligingscommissie geformeerd worden. Probeer vertegenwoordigers van zoveel mogelijk diensten en afdelingen in de commissie te laten plaatsnemen (zowel de hulpverleners als de ondersteunende diensten (de technische dienst, de interne dienst (receptie/portiers, etcetera)). Denk vooral ook aan vertegenwoordigers van plaatsen en diensten in de instelling die een verhoogd risico lopen zoals bijvoorbeeld in ziekenhuizen de Spoedeisende Hulp. Om een directe lijn naar de directie en het management te hebben, dient ook een lid van het managementteam deel te nemen aan de beveiligingscommissie. Daarnaast ook een vertegenwoordiger van de regiopolitie. Naast de inbreng van specifieke kennis kan deze functionaris als kontaktpersoon bij de regiopolitie optreden. Deelname van de politie geeft wederzijds vertrouwen. Alle partijen hebben het gevoel dat ze voor een gezamenlijk op te lossen c.q. aan te pakken probleem staan.

Taken interne beveiligingscommissie:

- onder voorzitterschap van de interne projectcoördinator begeleiden en eventueel uitvoeren van beveiligingsactiviteiten
- het vervullen van een schakelfunctie naar de overige medewerkers in de organisatie
- het opstellen van een integraal beveiligingsbeleidsplan.

De voorwaarden voor functioneren van de interne beveiligingscommissie komen in grote lijnen overeen met de eerder omschreven voorwaarden van de regionale projectgroep.

Interne projectcoördinator

De taken van de interne projectcoördinator zijn vergelijkbaar met die van de projectcoördinator maar dan specifiek gericht op de eigen instelling.

37

4.2.3 Het maken van een projectplan

Waarom een projectplan ?

Kenmerkend voor een projectmatige aanpak is dat in een vooraf bepaalde tijd, met specifiek voor dat doel beschikbaar gestelde middelen, duidelijk omschreven doelstellingen gerealiseerd worden.

Er wordt gewerkt met een duidelijke fasering van activiteiten. Dit wil zeggen dat alle projectactiviteiten die noodzakelijk zijn om het gewenste resultaat te bereiken, in logische stappen worden verdeeld. Tevens zorgt een goede planning ervoor dat van begin tot eind van het project bepaalde gespecificeerde beslissingen op de juiste plaats in het project plaats vinden. Dit alles wordt in een projectplan beschreven. Het plan heeft dan ook een ondersteunende functie ten behoeve van de activiteiten die gericht zijn op de fasering en beheersing van het project. Daarnaast geeft het plan de beslismomenten aan en de wijze waarop diverse belanghebbenden over de voortgang worden geïnformeerd.

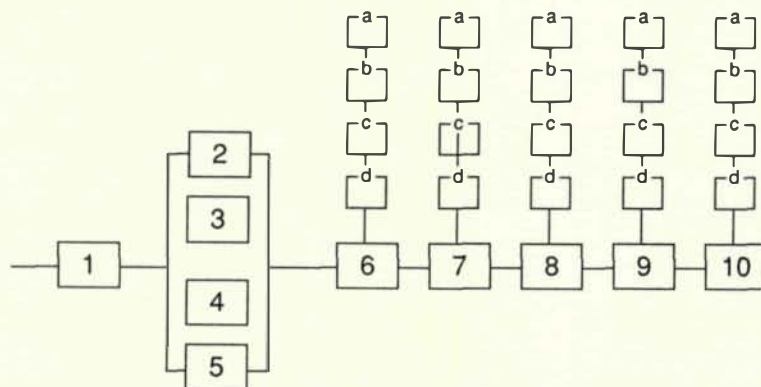
Een goed hulpinstrument daarbij vormt de zogeheten netwerkplanning.

Netwerkplanning is een hulpmiddel om een projectplan zo vorm te geven dat men heel snel kan zien in welke volgorde de activiteiten uitgevoerd dienen te worden.

Een netwerkplan bevat

- alle activiteiten die bij de uitvoering van het project dienen te worden ondernemen; wie de activiteiten uitvoert, wanneer en in hoeveel tijd
- de volgorde van de activiteiten in hun onderlinge relatie (voor C dienen A en B gedaan te zijn en na C volgen tegelijkertijd D, E en F etcetera)
- een tekening van het voorgaande waarbij elke activiteit wordt weergegeven door een hokje (met informatie over de desbetreffende activiteit) en waarbij de relaties tussen de activiteiten zijn aangegeven.

Op de volgende bladzijde is een voorbeeld van een netwerkplanning weergegeven.



a = instelling 1

c = instelling 3

b = instelling 2

d = instelling 4

1 = Start-vergadering Regionale Beveiligingscommissie

2 = Installatie Interne Beveiligingscommissies instelling

3 = Project-start: ondertekening samenwerkingsconvenant

4 = Aankondiging/informatie aan personeel instellingen

5 = Informatie aan pers

6 = Regionale projectgroepvergadering: voorbereiding personeelsenquete.

7 = Voorlichtingsbijeenkomsten binnen de betrokken instellingen

8 = Verspreiding personeelsenquete

9 = Inzameling van de personeelsenquetes

In een netwerkplan zijn dus in getekende vorm alle activiteiten in hun onderlinge samenhang opgenomen. Met dit netwerkplan kan een veel bredere groep mensen (inclusief de mogelijke uitvoerders) inzicht krijgen in het project. Het netwerkplan dient dan ook - naast een planningstechnisch doel - vooral als een communicatie-instrument gezien te worden.

Inhoud projectplan

Het is zaak te zorgen voor een helder projectplan waartegen directie en management ja kunnen zeggen.

Dit plan kan de volgende punten bevatten:

- de motieven voor het project
(de samenvattende informatie over de problemen en achtergronden)
- de doelstellingen van het project
- de begin- en einddatum van het project
- de te ondernemen stappen en acties
- de wijze waarop, wanneer en na welke stappen de organisatie geïnformeerd wordt over de voortgang van het project

- met welk doel en door wie gegevens ten behoeve van het project worden verzameld, verwerkt en beheerd
- de condities.

In bijlage 1 treft u een voorbeeld aan van een projectplan.

4.2.4 De formele vaststelling van het plan van aanpak

De formele vaststelling van het plan van aanpak door de directie is de laatste stap in deze eerste, voorbereidende fase.

De vaststelling van het plan van aanpak vormt het moment waarop het personeel nader geïnformeerd wordt. U kunt de medewerkers inlichten via een artikel in het personeelsblad of in een circulaire.

Met het oog op het ontwikkelen van draagvlak binnen de organisatie en een preventie-cultuur is het noodzaak om de organisatie van begin af aan en op vaste momenten tijdens het project te informeren over zaken als criminaliteitsrisico's, de incidenten die zich voordoen, welke beveiligingsmaatregelen getroffen zijn, welke voortgang en resultaten geboekt worden. In de verdere beschrijving van het projectverloop zullen wij dit aspect steeds benadrukken. In bijlage 7 is een voorbeeld van een communicatieplan opgenomen waarin wordt aangegeven op welke wijze en op welke momenten in het project aandacht besteed dient te worden aan voorlichting.

Nu het plan van aanpak formeel goedgekeurd is en de medewerkers zijn geïnformeerd, kan de tweede fase waarin het veiligheidsonderzoek plaatsvindt, van start gaan.

4.3 De analyse-fase: het veiligheidsonderzoek

Het veiligheidsonderzoek heeft tot doel de huidige stand van zaken op het gebied van beveiliging en onveiligheid binnen de instelling in kaart te brengen. In deze handleiding worden vier instrumenten besproken:

- 1 de incidentenregistratie
- 2 de kleurenmethode
- 3 de personeelsenquête.
- 4 de security audit

Met behulp van deze instrumenten kunnen gegevens verzameld worden over

- de aard en omvang van de problematiek
- de bestaande onveiligheidsgevoelens en -ervaringen
- de potentiële risico's van instellingen en de sterke en zwakke kanten van de beveiliging.

Als de methoden in combinatie met elkaar worden gebruikt, kunnen de uitkomsten dienen als concrete aanzet voor een beveiligingsbeleid en directe aanwijzingen tot verbeteringen van de beveiliging in en rond de instelling opleveren.

4.3.1 De incidentenregistratie

Onderbouwing met geregistreerde criminaliteitscijfers vormt het fundament van een goed beveiligingsbeleid (meten is weten). De praktijk leert dat incidentenregistraties binnen instellingen nog weinig ontwikkeld zijn. De procedures zijn vaak onduidelijk en lang niet iedereen binnen de instelling is op de hoogte van het bestaan van een incidentenregistratie. Bovendien blijken de registratiegegevens veelal niet vergelijkbaar te zijn met en afgestemd op die van de regiopolitie. Het is dus zaak een goede incidentenregistratie op te zetten met duidelijke, binnen de instelling bekende procedures

waarin ook de controle op de naleving van de regels rond de incidentenmelding geregeld wordt. Van groot belang is dat alle als 'incident' omschreven voorvallen uniform en op één plaats worden geregistreerd.

Ontwerp in overleg met de politie in uw regio een incidentenregistratieformulier of pas het bestaande formulier aan. Probeer tevens te komen tot een vereenvoudigde aangifteprocedure.

U kunt de volgende maatregelen voorstellen:

- het gebruik van een gezamenlijk onderling afgestemd registratieformulier van politie en instelling; (zie in bijlage 6 een voorbeeld registratieformulier)
- het creëren van een centraal meldingspunt incidenten in de instelling waar het personeel, de patiënten en de bezoekers aangifte kunnen doen
- een daartoe aan te wijzen instellingsfunctionaris wordt belast met het invullen van het formulier
- de formulieren worden door de politie (bijvoorbeeld de wijkagent), in de hoedanigheid van opsporingsambtenaar, mede ondertekend
- de gegevens worden ondergebracht in het politieb Bestand en in een apart instellingsbestand
- vanuit de regiopolitie wordt overleg gepleegd met het Openbaar Ministerie met het verzoek of dat het registratieformulier en de te volgen procedure wil legitimeren. Het resultaat is dat de incidentmelding de status krijgt van een aangifte bij de politie. De verzamelde gegevens zijn op deze wijze volledig en vergelijkbaar en kunnen voor de instellingen en regiopolitie beleidsrelevante informatie verschaffen.

Het management wordt via het managementoverleg op de hoogte gesteld van de afspraken met de politie en de te volgen procedure.

Het personeel wordt via het personeelsblad en binnen de bestaande overlegkaders geïnformeerd over het belang van het melden van incidenten en over de nieuwe afspraken.

Patiënten/cliënten worden via een voorlichtingsbrochure en/of het videonet van de instelling op de hoogte gesteld.

Om de motivatie voor beveiliging op peil te houden, worden het management en de rest van het personeel op vaste tijden geïnformeerd over de resultaten van de incidentenregistratie via de net genoemde kanalen.

4.3.2 De kleurenmethode

De kleurenmethode is een methode waarbij op plattegronden van het gebouw met kleuren de knelpunten in de beveiliging worden aangegeven. In bijlage 1 is een uitgebreide beschrijving van de werkwijze van de kleurenmethode opgenomen. Hier wordt slechts kort op de methode ingegaan.

Op twee plattegronden wordt achtereenvolgens met behulp van kleuren (die van groen naar rood lopen) aangegeven:

- a de mogelijke kwetsbaarheid, als gevolg van criminele handelingen aan personen, goederen of bedrijfsprocessen (van "zeer kwetsbaar" tot "niet kwetsbaar") in het gebouw, de afdeling en ruimten
- b de toegankelijkheid van het gebouw, de afdeling en ruimten voor criminele acties voor genode en ongenode bezoekers aan te geven (van "zeer hoge drempel" tot "geen drempel").

Door vergelijking van beide plattegronden worden de criminele risico's en het niveau van de (fysieke) beveiliging daartegen in een gebouw zichtbaar. Bijvoorbeeld een zeer

kwetsbaar goed (rood) in een ruimte zonder drempel (groen). Grote kleurverschillen dienen aangepakt te worden. Ook kunnen de in het kader van de beveiliging genomen maatregelen met behulp van de kleurenmethode worden geëvalueerd.

De kleurenmethode is vooral geschikt om zicht te krijgen op concrete criminele risico's als diefstal of vernieling van waardevolle goederen in het bedrijfsgebouw. De aan de hand van de kleurenmethode gevonden oplossingen zitten dan ook vooral op de zogenaamde lagere beveiligingsniveaus van keuze en installatie van middelen. Informatie over het gevoerde beveiligingsbeleid en beveiligingscultuur kunnen niet via de kleurenmethode aangegeven worden.

De kleurenmethode is een goed en eenvoudig toe te passen instrument. De uitvoering vraagt echter wel een flinke tijdsinvestering. De praktijk leert echter dat deze investering zeker geen weggegooid geld is. Integendeel. Door toepassing van de kleurenmethode wordt een duidelijk en overzichtelijk beeld verkregen van de beveiligingssituatie van een gebouw. De hiaten en knelpunten daarin worden duidelijk en daarmee ook de oplossingsmogelijkheden. Dat geldt niet alleen voor de beveiligingsfunctionaris maar ook voor de afdelingsleiding, die bij de invulling van de kleurenmethode betrokken wordt. De kleurenmethode is ook bij uitstek een discussie-instrument omdat duidelijk kan worden dat de ene functionaris risico's en drempels anders inschat dan een ander.

41

De kleurenmethode-procedure

De stappen bij de kleurenmethode

1 Voorbereiding

- organisatie regelen (coördinatie, contactpersoon, uitvoering en dergelijke)
- het plan de campagne opstellen
- zorgen voor bruikbare plattegronden van het gehele gebouw.*

2 Voorlichting aan de uitvoerders en leidinggevendenden

- toelichting op de methode en de begrippen
- instructiebijeenkomst over wie/hoe/wanneer de methode wordt uitgevoerd
- voorlichting aan het personeel in het personeelsblad.

3 Uitvoering

- invullen van de twee plattegronden door de uitvoerders in overleg met leidinggevendenden
- verwerking van de gegevens.

4 Analyse in de beveiligingscommissie

- risico-analyse van kleurverschillen in mogelijke kwetsbaarheid en toegankelijkheid
- trekken van conclusies en formuleren van adviezen.

5 Rapportage van bevindingen

- schriftelijke rapportage door de projectcoördinator in samenwerking met de uitvoerders
- presentatie van de resultaten in het managementteam
- informatie aan medewerkers in het personeelsblad.

Het toepassen van de kleurenmethode kan zowel door medewerkers van de instelling (leden van de beveiligingscommissie) als door derden gedaan worden.

Het voordeel om de kleurenmethode in eigen beheer uit te voeren is dat medewerkers bekend zijn met het gebouw en daardoor meer grip op het geheel kunnen houden. De kleurenmethode kan echter ook door anderen uitgevoerd worden, bijvoorbeeld door studenten bouwkunde. De daaraan verbonden kosten hoeven niet bijzonder hoog te zijn. In beide gevallen zijn een goede begeleiding en instructie van de uitvoerders nodig.

* Bij hoogbouw kan het voorkomen dat alle etages qua inrichting/functie gelijk zijn maar het is beter hier niet van uit te gaan.

4.3.3 De personeelsenquete

Het houden van een enquête onder de personeelsleden van een instelling heeft tot doel een scherper beeld te krijgen van de (on)veiligheid in en rondom de instelling, het slachtofferschap onder medewerkers en het bestaan van subjectieve gevoelens van onveiligheid. De personeelsenquete is een noodzakelijke aanvulling op de registratiegegevens en bevordert de betrokkenheid van de medewerkers bij beveiliging.

De personeelsenquete-procedure

1 Voorbereiding

Beleg een bespreking van de beveiligingscommissie om de volgende zaken te bepalen:

- De inhoud van de personeelsenquete.
Het opstellen van enquêtes is een vak apart. In de projecten in Utrecht, Twente en Flevoland zijn varianten gebruikt van de personeelsenquete uit de publicatie "Beveilig het ziekenhuis, Preventie in een klantgerichte gatenkaas" (1991). Daarin staan veel open vragen wat verwerkingsproblemen geeft als de enquête in grote aantallen uitgaat. Als bijlage 4 is een bijgewerkte versie ingesloten. Het is natuurlijk mogelijk dat u een enquête opstelt die precies is afgestemd op de specifieke situatie van uw instelling. Ook kunt u aansluiting zoeken bij de door de politie gebruikte standaardenquête "Politie-monitor". Als u zelf de enquête opstelt is het goed om deze te laten beoordelen door een onderzoekskundige en in elk geval door degene die de gegevens verwerkt. Het is in dat geval aan te bevelen een proefenquête te houden. Personeelsenquetes kunnen een dankbaar stage-object zijn voor studenten (ten minste op HBO-niveau).
- De wijze van verspreiding van de personeelsenquete.
Richt in ieder geval de enquête persoonlijk aan de medewerkers; Overweeg de enquête tegelijk met de salarisstroom van de medewerkers te verzenden. In de ziekenhuisprojecten Twente bleek dit een positief effect op de respons te hebben.
- Wie de personeelsenquete gaat verwerken.
- Wanneer de personeelsenquete wordt gehouden.
- Wanneer de personeelsenquetes ingeleverd dienen te zijn.
- Wie van de beveiligingscommissie de kontaktpersoon is voor de personeelsenquete.

2 Informeer de organisatie over de personeelsenquete

De personeelsenquete dient uiteraard voorafgegaan te worden door goede (schriftelijke en mondelinge) informatie. Dat zal de response aanzienlijk beïnvloeden. Doe een vooraankondiging over de te houden personeelsenquete in het personeelsblad. Leg daarin uit wat de personeelsenquete inhoudt en benadruk het belang van een hoge response.

Vertel wanneer men de enquête kan verwachten en vraag om een snelle reactie (binnen tien tot veertien dagen). Geef aan wie de kontaktpersoon in de beveiligingscommissie is wat betreft de personeelsenquête.

Zorg dat de personeelsenquête daarnaast ook besproken wordt in de bestaande overlegkaders.

3 Verwerk de gegevens zoals afgesproken in de beveiligingscommissie.

4 Bespreek de uitkomsten van de personeelsenquête in de beveiligingscommissie.

Hierna volgen de:

5 Rapportage.

De projectcoördinator draagt in samenwerking met de onderzoekers zorg voor de de rapportage van de personeelsenquête.

6 Presentatie resultaten personeelsenquête.

Het is goed om apart aandacht te besteden aan de resultaten van deze enquête. Uiteindelijk vormt de personeelsenquête samen met de resultaten van de incidentenregistratie, het gebouwenonderzoek op basis van de kleurenmethode en de security-audit (zie hierna), het basismateriaal voor het op te stellen beveiligingsplan. Maar een daaraan voorafgaande rapportage van de bevindingen in het personeelsblad is aan te bevelen.

4.3.4 De security-audit

Wat is een security-audit?

Een security-audit is een systematisch en onafhankelijk onderzoek naar de beveiliging (maatregelen en activiteiten) van een organisatie, waarbij wordt nagegaan in welke mate het beveiligingssysteem effectief is in het realiseren van objectieve en subjectieve veiligheid van mensen en eigendommen.

Doel van een audit

Doel van een security-audit is het verbeteren van het beveiligingssysteem en uiteindelijk het terugdringen, uitsluiten en voorkomen van onveilige situaties.

De activiteiten van een auditteam dienen zich dan ook te richten op:

- het geven van inzicht in de bestaande beveiligingsrisico's en de instelling de spiegel van de actuele beveiligingssituatie voor te houden
- het attenderen van het management en beveiligingsmensen op zaken die volgens het team met prioriteit aangepakt dienen te worden
- het aanzetten tot activiteiten die dienen te leiden tot een integraal beveiligingssysteem.

Wie zitten in een audit-team?

Een security-audit wordt uitgevoerd door gespecialiseerde onafhankelijke functionarissen die zowel over veldkennis als materie-deskundigheid beschikken. De functionarissen zijn afkomstig van buiten de organisatie of van buiten de werkeenheid waar de audit wordt uitgevoerd. Zij vormen zich een beeld van de kwaliteit van een (onderdeel) van de organisatie, in dit geval het aspect van beveiliging.

Procedure voor het houden van een audit

1 Voorbereidingsfase

- organisatie van de audit bepalen
- planning van de werkzaamheden maken
- selectie van de audit-teamleden
- documenten verzamelen (plattegronden, beleidsstukken over beveiliging, brochures, werkinstructies, formulieren, organisatie van de beveiliging).

2 Instructiebijeenkomst van het audit-team

- toelichting op doel en werkwijze van de instelling
- wanneer en hoe de audit plaatsvindt (dagprogramma)
- toegepaste methodieken
- vaststellen van de onderzoeksonderdelen/facetten
- te gebruiken hulpmiddelen (vragenlijst, interview, protocol, checklist). In bijlage 2 is een voorbeeld van een observatiechecklist opgenomen.
- wijze van werken (observeren, gesprekken, registreren)
- taakverdeling in verband met rapportage.

4 Informatie aan leidinggevend (mondeling door managementteam) en medewerkers (via personeelsblad).

5 Uitvoeren van de audit

In bijlage 2 is een voorbeeld van een dagprogramma opgenomen.

6 Verwerking van de gegevens

- concept-rapportage van audit-teamleden naar de project-coördinator
- verwerking in concept-tekst
- commentaren, aanvullingen, verbeteringen door teamleden
- eindverslag opstellen.

7 Rapportage

- eindverslag aan de directie aanbieden door de project-coördinator
- toelichting in managementteam; beleidsconclusies trekken
- personeel informeren over resultaten en beleidsvoornemens.

Het samenstellen van een auditteam blijkt in de praktijk geen lastige opgave. Collega's van andere instellingen en medewerkers van de politie willen doorgaans graag zo'n dienst verlenen. Temeer omdat het hen scherpert in hun eigen kennis op het gebied van de beveiliging.

Benader voor de samenstelling van het audit-team in elk geval collega's uit instellingen in de regio, een organisatiekundige, een politiefunctionaris en een beveiligingsdeskundige. Zorg dat het audit-team samengesteld is uit vier tot zes gemotiveerde en deskundige mensen die voldoende tijd beschikbaar hebben voor de audit. Geef enige weken van te voren aan de leden van het audit-team de vragenlijst en instructies ten behoeve van de audit en een plattegrond met een complete beschrijving van de gebouwen.

In bijlage 3 is een voorbeeld van een lijst met vragen gevoegd die tijdens een security-audit aan de orde dienen te komen.

Instrueer het audit-team van te voren niet in de 'deskundigenvalkuil' te vallen. Deze valkuil houdt in dat zaken die door het auditteam als minder goed beoordeeld worden,

noodzakelijkerwijs ook door een instelling aangepakt moeten worden. De directie van een instelling moet zelf beslissen of zij iets gaat doen of niet. Het kan bijvoorbeeld zijn dat een auditteam een instelling wel wat al te open vindt maar dat dit juist een beleidslijn van de directie is die sommige risico's daarbij incalculeert.

4.4 De beleidsfase

4.4.1 Het vaststellen van maatregelen en middelen

De uitkomsten van het veiligheidsonderzoek kunnen verwerkt en gecategoriseerd worden onder de elementen van het preventiewiel:

- hoe staat het met het beveiligingsbeleid; welke visie heeft men
- hoe staat het met de organisatorische condities, welke procedures werken wel/niet
- welke voorzieningen zijn getroffen en hoe effectief zijn deze
- wat is te zeggen over de beveiligingscultuur.

45

De resultaten uit de vier deelonderzoeken zullen de knelpunten in elk van de elementen zichtbaar maken.

De knelpunten kunnen doorgaans nooit allemaal direct opgelost worden. Er zullen prioriteiten moeten worden gesteld voor wat betreft de te nemen maatregelen en in te zetten middelen. Het stellen van prioriteiten wordt onder andere bepaald door:

- de urgentie van de oplossing van knelpunten
- de mogelijkheden (middelen) die de instelling heeft om de knelpunten op te lossen
- de ervaring die men heeft met beveiligingsplannen.

4.4.2 Het schrijven van een beveiligingsbeleidsplan

Een beveiligingsbeleidsplan

Een onmisbaar instrument in het beveiligingsproces vormt het beveiligingsbeleidsplan. In dit plan wordt de visie van de instelling op beveiliging alsmede de maatregelen en middelen vastgelegd. Het vormt het sluitstuk van de analyse van de beveiligingssituatie. Na goedkeuring van het plan door de directie kan tot uitvoering van de maatregelen overgegaan worden.

Inhoud van een beveiligingsbeleidsplan

1 De aanleiding

In dit hoofdstuk worden de organisatie, de aanleiding, de motieven en de aanpak voor het project om te komen tot een beveiligingsbeleidsplan beschreven.

2 De resultaten van het veiligheidsonderzoek.

Dit hoofdstuk beschrijft de resultaten van de vier onderzoeksinstrumenten (de incidentenregistratie, de personeelsenquête, de kleurenmethode en de security-audit) en de belangrijkste conclusies die de instelling daaruit dient te trekken. De gegevens van het onderzoek dienen als voormeting of nulmeting. De effecten van te nemen maatregelen kunnen te zijner tijd afgemeten worden aan het verschil tussen deze voormeting en uit te voeren nameting.

3 De te realiseren beleidsopgaven.

In deze paragraaf wordt op basis van de uitkomsten van het veiligheidsonderzoek aangegeven welke doelen op wat langere termijn de instelling zich zal stellen voor wat betreft verbeteren van de beveiliging alsmede de prioriteiten daarin. Dit veronderstelt

dat het managementteam de voorstellen die de beveiligingscoördinator heeft gedaan, tot het zijne maakt en daarin prioriteiten bepaalt.

4 De te realiseren maatregelen

Deze paragraaf bevat een beschrijving van de concrete maatregelen en middelen als de instelling de beleidsopgaven wil realiseren. Met het oog op de later uit te voeren evaluatie naar de effectiviteit van deze maatregelen en middelen dienen de doelen uit punt 3 hiervoor concreet, haalbaar en meetbaar geoperationaliseerd te worden.

5 Wie is verantwoordelijk voor de uitvoering en de coördinatie

Dit hoofdstuk beschrijft de taken, bevoegdheden en verantwoordelijkheden van de betrokkenen bij de uitvoering en de coördinatie van het beveiligingsbeleidsplan.

6 Welke middelen zijn beschikbaar.

In dit hoofdstuk wordt aangegeven welke financiële middelen en mensuren beschikbaar dienen te zijn ten behoeve van de uitvoering van de vastgestelde beveiligingsmaatregelen.

7 Wanneer moeten de maatregelen zijn uitgevoerd.

Dit hoofdstuk geeft het tijdspad aan waarbinnen de maatregelen dienen te zijn uitgevoerd.

8 De wijze van evaluatie

In dit hoofdstuk wordt aangegeven op welke wijze, op welke termijn en door wie de evaluatie uitgevoerd gaat worden.

4.5 De uitvoerings- en evaluatiefase

De uitvoeringsfase is ongetwijfeld de lastigste fase bij het uitvoeren van de maatregelen zoals die in het beveiligingsbeleidsplan worden genoemd. Dan komt het aan op echt managen: "getting things done, through people". En pas daarna komt het meest veronachtzaamde onderdeel van goede projectvoering aan de orde; de evaluatie.

Evaluatie van de maatregelen is nodig om waar mogelijk bij te kunnen sturen en te leren van gemaakte fouten. Vaak denkt men pas helemaal aan het eind van het traject, als de maatregelen al uitgevoerd zijn, aan evaluatie. Het verdient echter ten zeerste aanbeveling om de evaluatie in te bedden in de planning van het project en wel in een zo vroeg mogelijk stadium. Tijdens het veiligheidsonderzoek wordt informatie verzameld die dienst kan doen als zogenaamde nul- of voormeting. Deze gegevens kunnen later afgezet worden tegen de gegevens die u na afloop van het project verzamelt. In de uitvoeringsfase formuleert u op basis van de onderzoeksresultaten beveiligingsdoelen. Deze doelen dienen vertaald te worden in begrippen die meetbaar zijn. Doelen waarvan niet gemeten kan worden of en in hoeverre zij gehaald zijn, kunnen immers niet geëvalueerd worden.

Voor de effect-evaluatie is de zogeheten doel-middelen keten van belang, omdat het effect van het project uiteindelijk afgemeten dient te worden aan de mate waarin het hoofddoel is bereikt.

Een voorbeeld

Als doelstelling kan geformuleerd worden: 'Het ontwikkelen van een beveiligingsattitude bij medewerkers'.

Subdoelen daarvan zijn bijvoorbeeld als volgt te omschrijven:

- toename van probleembesef bij medewerkers
- bekendheid vergroten met beveiligingsprocedures
- afsluitgedrag van medewerkers verbeteren.

Als middelen kunnen geformuleerd worden:

- voorlichtingsbijeenkomsten in september voor het personeel over criminaliteitsrisico's en incidenten
- artikelenreeks in het informatieblad voor het personeel over incidenten, ervaringen en te volgen procedures
- hoofd beveiliging verzorgt een dagdeel in de introductiebijeenkomst en de inserviceopleiding
- bewakingspersoneel registreert resultaten van sluitronde en rapporteert twee-maandelijks aan de afdelingsleiding.

De resultaten kunnen als volgt gemeten worden:

- ontwikkeling in de registratiecijfers
- jaarenquete bij a-selecte groep medewerkers over bekendheid en ervaringen met beveiligingsprocedures.

Op grond van de evaluatie worden indien noodzakelijk de beleidsopgaven bijgesteld, nieuwe beleidsopgaven geformuleerd en een beveiligingsbeleidsplan voor het volgende jaar opgesteld.

Het is belangrijk om in een vroeg stadium vast te stellen wat voor soort evaluatie u gaat doen. Voor een proces-evaluatie moet u namelijk vaak andere methoden gebruiken dan voor een effect-evaluatie.

N.B. Bij het Ministerie van Justitie is de zogeheten Stappenschijf te bestellen. De Stappenschijf kan u behulpzaam zijn bij het opzetten van een evaluatie. Onderdeel van het programma van de Stappenschijf is een systematische beschrijving van de stappen die u moet zetten bij een proces- of effectevaluatie van een project.

Bijlage 1 voorbeeld van een projectplan

49

Het projectplan kan de volgende punten bevatten:

1 De motieven

Beschrijving van samenvattende informatie over de problemen en achtergronden.

2 Begin- en einddatum van het project

3 De doelstellingen

Bijvoorbeeld:

- het verminderen van onveiligheidsgevoelens bij medewerkers, patiënten en bezoekers van de (participerende) instelling(en)
- het verlagen van de geregistreerde criminaliteit, dan wel deze op een minimum peil te houden
- het stroomlijnen van het aangiftebeleid
- het tot stand brengen van een beveiligingsattitude binnen de (deelnemende) instelling(en) middels
 - vergroting van het bewustzijn bij het management, medewerkers, patiënten en bezoekers, inzake de eigen verantwoordelijkheid voor de objectieve en subjectieve veiligheid van personen en voor de veiligheid van persoonlijke- en instellingseigendommen.
 - het vergroten van de doeltreffendheid en doelmatigheid van de reeds getroffen en nog te treffen maatregelen en het verhogen van de kwaliteit van de dienstverlening.

4 Conditie

Bijvoorbeeld:

- De instelling is bereid tot het houden van een gezamenlijk regionaal project met andere instellingen en tekent daartoe een samenwerkingsconvenant.
- De instelling gaat akkoord met het instellen van een regionale projectgroep.
- De instelling benoemt een interne projectcoördinator.
- De instelling stelt een interne beveiligingscommissie in.
- De instelling verplicht zich tot het houden van de intern uit te voeren activiteiten, gericht op de realisering van het beveiligingsbeleidsplan i.c. schept de voorwaarden daarvoor.
- De instelling verklaart zich bereid om de resultaten van het project in de vorm van intern dan wel gezamenlijk uit te voeren maatregelen, serieus in overweging te nemen. Ook wanneer dat budgettaire consequenties heeft.

- De instelling stelt financiële middelen beschikbaar ten behoeve van het project aan te wenden voor
 - de financiering van personeelskosten voor het projectsecretariaat
 - financiering van bijzondere activiteiten (voorlichting, gegevensverwerking, kopieerkosten, verblijfs- en conferentiekosten etcetera).
- De projectcoördinator is tevens budgetbeheerder.
De instelling draagt zorg voor organisatorische ondersteuning in de vorm van een project-assistent.

5 De stappen en acties

Datum/Periode

50

- Eerste bijeenkomst van de (Regionale) Projectgroep.
 - Instellen van de Interne Beveiligingscommissie.
 - Ondertekening van het samenwerkingsconvenant: formele start van het project.
 - Aankondiging en informatie aan het personeel.
 - Informatie aan de pers
- Tweede Bijeenkomst van de (Regionale) Projectgroep.
Agendapunten:
 - Hoe dient het personeel voorgelicht te worden?
 - Voorbereiding incidentenregistratie.
 - Voorbereiding personeelsenquete.
 - Voorlichtingsbijeenkomsten in de instellingen.
 - Drukken formulieren personeelsenquete.
 - Verspreiding formulieren personeelsenquete.
 - Inzamelen ingevulde personeelsenquetes.
 - Verwerking van de gegevens van de personeelsenquetes.
 - Opstellen rapportages uitkomsten van de personeelsenquetes.
 - Terugkoppeling uitkomsten aan directie, management en personeel.
- Derde bijeenkomst van de (Regionale) Projectgroep.
Agendapunten:
 - Verzamelen gegevens instelling(en) (geregistreerde criminaliteit).
 - Verzamelen gegevens politie (geregistreerde criminaliteit).
 - Voorbereiding kleurenmethode.
 - Ten behoeve van de uitvoering van de kleurenmethode:
 - Verzamelen van plattegronden van de instellingen .
 - Indelen van de gebouwen.
 - Maken van lijsten/plattegronden instellingen voor hoofden.
 - Ophalen van lijsten/plattegronden bij hoofden.
 - Inkleuren plattegronden/schema's instellingen.
 - Voorbereiding security-audit door team van deskundigen.
 - Uitvoering audits in de instellingen.
 - Rapportage audits.
 - Voorlichtingsbijeenkomst personeel: informatie stand van zaken van project.
- Vierde bijeenkomst van Regionale Projectgroep.
Agendapunten:
 - Opstellen van beveiligingsbeleidsplannen.
 - Voorbereiden bijeenkomst van directies waar beveiligingsbeleidsplannen worden aangeboden.
 - Vaststelling van beveiligingsbeleidsplannen door directies.
 - Informeren van personeel over beveiligingsbeleidsplan.

Bijlage 2 voorbeeld van een dagprogramma van een security audit observatiechecklist

51

Voorbeeld dagprogramma

07.45 uur	Aankomst entree instelling.
08.00 - 08.45 uur	Observatie instroom van personeel: - hoofdingang - parkeerterrein - fietsenstalling.
09.00 - 09.30 uur	Gesprek hoofd algemene zaken aan de hand van onderdelen van de vragenlijst van het Preventiewiel.
09.45 - 10.00 uur	Koffie en taakverdeling Subgroepen (koppels) met behulp van plattegrond.
10.00 - 12.00 uur	Rondlopen en gesprekken met medewerkers (observatie van feiten en uitwisselen van interpretaties).
12.00 - 13.30 uur	Lunch met - evaluatie morgenactiviteit - taakverdeling middag.
13.30 - 14.00 uur	Gesprek met beveiligingsfunctionaris.
14.00 - 16.00 uur	Observatie in koppels.
16.00 - 17.00 uur	Gegevens uitwisselen en conclusies trekken ten behoeve van rapportage.

Observatiechecklist

Buitenschil

Let hierbij op:

- afstand tot het gebouw
- verlichting/overzichtelijkheid (bebossing)
- toegankelijkheid voor derden

- . parkeervoorzieningen
- . fietsenstalling
- . toegangswegen
- . route tussen gebouwen
- . omheining (toegankelijk? sterk?)

- . groenvoorziening (hoogte/camouflerend?)
- . gevel (opklim-mogelijkheden)
- . stortplaats.

Binnenschil

- Let hierbij op:
- openingen (ramen, deuren, gangen, nooduitgangen)
 - afsluitsystemen (sloten en dergelijke)
 - toegankelijkheid (fysiek en psychisch: hoe reageert men op bezoekers)

52

- . receptie
- . garderobes (bezoekers/personeel)
- . spoedeisende hulp
- . intensive care
- . kinderafdeling
- . personeelsrestaurant
- . verpleegafdelingen (medicijnkast, medisch archief, kluisjes, garderobekast)
- . afsprakenbureau op de poli
- . administratie (beveiliging computers, kluis)
- . medische dossiers
- . magazijn
- . technische dienst-ruimte
- . machinekamer(s)
- . keuken

Spelregels:

- eerst binnenlopen, reactie afwachten
- gesprek met eerst verantwoordelijke
- observatie uitvoeren
- bevindingen exact noteren
- later (gezamenlijk) interpreteren en conclusies trekken.

Bijlage 3 de kleurenmethode

53

De kleurenmethode*

De kleurenmethode is een techniek waarmee op basis van plattegronden en kleuren knelpunten in de beveiliging kunnen worden aangegeven. De kleurenmethode wordt gebruikt als hulpmiddel om de risico's in beeld te brengen, om na te gaan of de bestaande beveiliging afdoende is en om, in een later stadium, de genomen of geplande maatregelen te evalueren. De kleurenmethode is vooral geschikt om zicht te krijgen op concrete criminele risico's als diefstal of vernieling van waardevolle goederen in het bedrijfsgebouw. De aan de hand van de kleurenmethode gemaakte analyse heeft vooral betrekking op de keuze en installatie van middelen en het gebruik van beveiligingsmiddelen.

De bedrijfsdoelen, bedrijfsbeleid, bedrijfscultuur en risicobewustzijn, kunnen niet via de kleurenmethode opgespoord worden.

Werkwijze kleurenmethode

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

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

* Overgenomen uit Beveiliging bedrijfsvestigingen, Landelijk Bureau Voorkoming Misdrijven, 's Gravenhage, oktober 1992

De bedrijfsprocessen-plattegrond: kwetsbaarheid

De bedrijfsprocessen-plattegrond geeft inzicht in de plaats en routing van de belangrijkste procesgoederen (spullen, informatie, geld, etcetera) en procesmiddelen (productiemiddelen als machines, gereedschap, computers) binnen het gebouw. Daarbij wordt met kleuren aangegeven hoe kwetsbaar deze goederen/middelen zijn. Er wordt nog geen rekening gehouden met de aanwezige beveiliging, dat komt aan de orde in de beveiligingsplattegrond.

De relatieve kwetsbaarheid van goederen en middelen wordt gemeten via:

- de waarde voor de organisatie: de gevolgen die voor de organisatie ontstaan als een goed of middel verdwijnt of in het ongereede raakt (afbreukrisico);

- de 'criminele waarde': de aantrekkelijkheid van de goederen en middelen voor een potentiële crimineel.

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

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

tekening bedrijfsprocessen-plattegrond van een instelling

54

rood	zeer kwetsbaar/zeer aantrekkelijk
oranje	vrij kwetsbaar/vrij aantrekkelijk
groen	niet kwetsbaar/niet aantrekkelijk

Toelichting voorbeeld van de bedrijfsprocessen-plattegrond

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

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

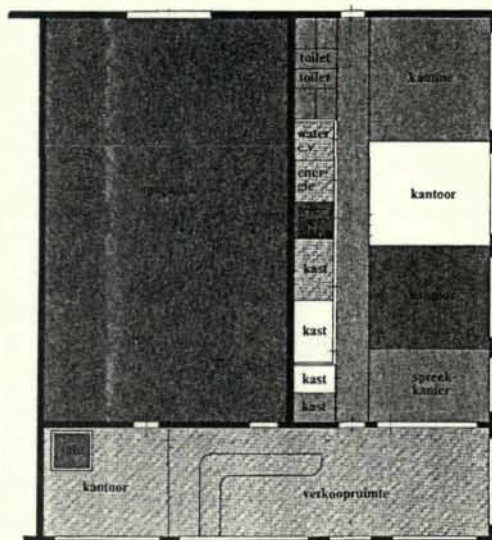
Beveiligingsplattegrond: bestaande drempels

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

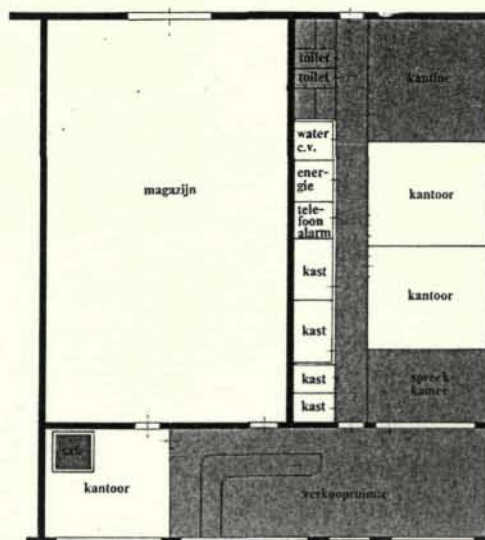
Op de bedrijfsplattegrond beteken de drie kleuren het volgende:

rood	zeer hoge drempel
oranje	hoge drempel
groen	geen drempel

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



figuur: bedrijfsprocessen-plattegrond



figuur beveiligingsplattegrond

In de tekening van de bedrijfsprocessen-plattegrond is aangegeven hoe kwetsbaar de verschillende ruimtes zijn en in de tekening van de beveiligingsplattegrond is de toegankelijkheid van de verschillende ruimtes aangegeven.

Risico-analyse: combinatie van bedrijfsprocessen- en beveiligingsplattegrond

Vergelijking van de twee plattegronden geeft bij kleurverschillen op (onderdelen van) de plattegrond een risico weer en geeft daarmee een aanzet voor verdere analyse. Met name de plaatsen waar de kleurverschillen groot zijn, verdienen extra aandacht, bijvoorbeeld rode voorwerpen (zeer kwetsbare/aantrekkelijke spullen) in een voor het publiek toegankelijke (= groene) ruimte. Of andersom, een stapel folders die in de kluis bewaard wordt (groene voorwerpen in een rode ruimte). Op het eerste gezicht lijkt dit laatste voorbeeld niet zo alarmerend. Het kan echter wel als consequentie hebben dat de kluis vaker open moet dan strikt noodzakelijk is. Bovendien wordt de aanwezige beveiliging op een onevenredige manier benut.

De risico-analyse spitst zich toe op twee vragen:

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

Gevonden kleurverschillen worden daarbij als volgt geïnterpreteerd:

Bedrijfsprocessen-plattegrond

		groen	oranje	rood
Beveiligings-plattegrond	groen	O.K.	te laag beveiligd/	
	oranje	oneconomische	O.K.	aandachtspunt
	rood	beveiliging		O.K.

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

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

De oplossing die men vindt kan heel goed bestaan uit een mix van deze beide benaderingen. In de praktijk zijn er natuurlijk altijd grenzen aan de mogelijkheid om

bedrijfsprocessen en bedrijfsgoederen te verplaatsen (de nieuwe indeling moet wel werkbaar blijven voor het personeel) en aan de mogelijkheid om bepaalde bedrijfsruimtes te beveiligen (sommige ruimtes moeten nu eenmaal zeer toegankelijk zijn). Het verdient aanbeveling om de gevonden oplossingen weer uit te zetten op twee plattegronden: zo kan men directanschouwelijk maken of de nieuwe situatie inderdaad een verbetering is. Mogelijk vindt men nieuwe knelpunten, die weer om een oplossing vragen.

Bijlage 4 de personeelsenquete

57

Personeelsenquete

persoonlijke gegevens

1. Wat is uw leeftijd?

- ☐ jonger dan 20 jaar
- ☐ tussen 20 en 29 jaar
- ☐ tussen 30 - 39 jaar
- ☐ tussen 40 en 49 jaar
- ☐ 50 jaar en ouder

2. Wat is uw geslacht?

- ☐ man
- ☐ vrouw

3. In welke functie bent u werkzaam?

- | | |
|--|---|
| ☐ medisch | ☐ was- en linnendienst |
| ☐ verzorgend | ☐ huishoudelijke dienst |
| ☐ verplegend | ☐ keuken |
| ☐ stafdiensten | ☐ buffet/restaurant |
| ☐ directie | ☐ anders, namelijk |
| ☐ paramedisch | |
| ☐ techniek/onderhoud | |
| ☐ receptie | |
| ☐ secretariaat/administratief | |

4. Op welke tijden bent u **meestal** werkzaam? (gaarne uw antwoord in één categorie aangeven)

- ☐ 's ochtends
- ☐ 's middags
- ☐ overdag (= 's ochtends en 's middags)
- ☐ 's avonds
- ☐ 's nachts
- ☐ 's avonds en 's nachts
- ☐ wisseldiensten

Veiligheidsgevoelens

5. 's Avonds en 's nachts kun je gerust alleen de instelling verlaten'.

- ☐ daar ben ik het mee eens
- ☐ daar ben het noch mee eens/noch mee oneens
- ☐ daar ben ik het niet mee eens
- ☐ vraag niet van toepassing op mijzelf (alleen dagdiensten)

6. 's Avonds en 's nachts kun je gerust alleen door de instelling lopen'.
- ☐ daar ben ik het mee eens
 - ☐ daar ben het noch mee eens/noch mee oneens
 - ☐ daar ben ik het niet mee eens
 - ☐ vraag niet van toepassing op mijzelf (alleen dagdiensten)
7. 'In de instelling bestaan plekken waar ik 's avonds en 's nachts liever niet alleen kom'.
- ☐ daar ben ik het mee eens
 - ☐ daar ben het noch mee eens/noch mee oneens
 - ☐ daar ben ik het niet mee eens
 - ☐ vraag niet van toepassing op mijzelf (alleen dagdiensten)
8. 'Op de parkeerplaats en/of in de fietsenstalling ben ik 's avonds en 's nachts liever niet alleen'.
- ☐ daar ben ik het mee eens
 - ☐ daar ben het noch mee eens/noch mee oneens
 - ☐ daar ben ik het niet mee eens
 - ☐ vraag niet van toepassing op mijzelf (alleen dagdiensten)
9. Hoe vaak **denkt u** aan de mogelijkheid ooit zelf slachtoffer te worden van enige vorm van criminaliteit **op en rond** het terrein van de instelling?
- ☐ vaak
 - ☐ geregeld
 - ☐ soms
 - ☐ zelden
 - ☐ nooit (u kunt vraag 10 overslaan)
10. Aan welke locaties denkt u dan in het bijzonder (maximaal drie aankruisen)
- ☐ de bushalte
 - ☐ het parkeerterrein
 - ☐ de fietsenstalling
 - ☐ de openbare weg in de directe omgeving van de instelling
 - ☐ anders, namelijk
11. Aan welk delict denkt u dan in het bijzonder? (maximaal twee aankruisen)
- ☐ diefstal van fiets
 - ☐ diefstal van bromfiets
 - ☐ diefstal van motorfiets
 - ☐ beschadiging van fiets
 - ☐ beschadiging van bromfiets
 - ☐ beschadiging van motorfiets
 - ☐ diefstal van auto
 - ☐ diefstal uit auto
 - ☐ diefstal uit en tevens beschadiging van auto
 - ☐ beschadiging van auto
 - ☐ diefstal van geld of andere persoonlijke eigendommen
 - ☐ handtastelijkheden
 - ☐ geweld
 - ☐ bedreiging
 - ☐ anders, namelijk.....

12. Hoe vaak denkt u aan de mogelijkheid ooit zelf slachtoffer te worden van enige vorm van criminaliteit **binnen de instelling** ?

- ☐ vaak
- ☐ geregeld
- ☐ soms
- ☐ zelden
- ☐ nooit (u kunt vraag 13 en 14 overslaan)

13. Aan welke ruimten binnen de instelling denkt u dan in het bijzonder?

- ☐ gangen
- ☐ openbare ruimten
- ☐ werkplek
 - meer specifiek
 - ☐ patiëntenkamer
 - ☐ behandelkamer
- ☐ anders, namelijk

59

14. Aan welk delict denkt u dan in het bijzonder? (maximaal twee aankruisen)

- ☐ diefstal van geld of andere persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....

15. Maakt u vanwege woon-/werkverkeer gebruik van een vervoermiddel?

- ☐ ja, namelijk fiets
- ☐ ja, namelijk bromfiets
- ☐ ja, namelijk auto
- ☐ ja, namelijk motor
- ☐ nee (u kunt vraag 16 overslaan)

16. Parkeert u uw vervoermiddel op het terrein van de instelling?

- ☐ ja
- ☐ nee

Slachtofferschap

17. Bent u het afgelopen jaar (..... t/m) zelf slachtoffer geweest van één van de hieronder genoemde gebeurtenissen **binnen** de instelling?

(Het is aan te bevelen om voor deze periode het afgelopen kalenderjaar te nemen, 1 januari tot en met 31 december ...)

- ☐ nee (u kunt doorgaan naar vraag 23)
- ☐ ja

- ☐ diefstal van geld of andere persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....

aantal keren

.....
.....
.....
.....
.....

16. In welk(e) maand(en) vond(en) de gebeurtenis(sen) plaats?

- ☐ diefstal van geld of andere
persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....
.....

17. Waar heeft het voorval plaatsgevonden?

(Bent u meerdere malen slachtoffer geworden van een voorval gaarne
aangeven waar het **laatste** voorval heeft plaatsgevonden)

17.a Diefstal van geld of andere persoonlijke eigendommen

- ☐ patiëntenkamer
- ☐ behandelkamer
- ☐ dienstruimte
- ☐ elders, namelijk

17.b Handtastelijkheden

- ☐ patiëntenkamer
- ☐ behandelkamer
- ☐ dienstruimte
- ☐ elders, namelijk

17.c Geweld

- ☐ patiëntenkamer
- ☐ behandelkamer
- ☐ dienstruimte
- ☐ elders, namelijk.....

17.d Bedreiging

- ☐ patiëntenkamer
- ☐ behandelkamer
- ☐ dienstruimte
- ☐ elders, namelijk.....

17.e Anders, nl.....

- ☐ patiëntenkamer
- ☐ behandelkamer
- ☐ dienstruimte
- ☐ elders, namelijk.....

18. Ondervond u van dit voorval materiële (financiële) schade?

- ☐ Nee, (u kunt doorgaan naar vraag 20)
- ☐ Ja

19. Kunt u een schatting maken van de materiële schade die u en/of uw verzekering
daardoor geleden heeft?

f

20. Ondervond u van dit voorval ook enige vorm van immateriële schade ?

- ☐ Nee (u kunt doorgaan naar vraag 22)
- ☐ Ja

21. Welke vorm(en) van immateriële schade hebt u ondervonden?

(U mag meer dan 1 antwoord geven)

- ☐ angst
- ☐ gevoelens van onveiligheid
- ☐ woede
- ☐ wantrouwen
- ☐ anders, namelijk.....

22. Heeft u de gebeurtenis gemeld?

- ☐ nee
- ☐ ja, melding bij de instelling
- ☐ ja, aangifte bij de politie

61

23. Bent u het afgelopen jaar (..... t/m) zelf slachtoffer geweest van één van de hieronder genoemde gebeurtenissen **in en rond** de instelling?

(Het is aan te bevelen om voor deze periode het afgelopen kalenderjaar te nemen, 1 januari tot en met 31 december ...)

- ☐ nee (u kunt doorgaan naar vraag 31)
- ☐ ja

- ☐ diefstal van fiets
- ☐ diefstal van bromfiets
- ☐ diefstal van motor
- ☐ beschadiging van fiets
- ☐ beschadiging van bromfiets
- ☐ beschadiging van motor
- ☐ diefstal van auto
- ☐ diefstal uit auto
- ☐ diefstal uit en beschadiging van auto
- ☐ beschadiging van auto
- ☐ diefstal van geld of andere persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....
-

24. In welk(e) maand(en) vond(en) de gebeurtenis(sen) plaats?

- ☐ diefstal van fiets
- ☐ diefstal van bromfiets
- ☐ diefstal van motor
- ☐ beschadiging van fiets
- ☐ beschadiging van bromfiets
- ☐ beschadiging van motor
- ☐ diefstal van auto
- ☐ diefstal uit auto
- ☐ diefstal uit en beschadiging
van auto
- ☐ beschadiging van auto
- ☐ diefstal van geld of andere
persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....
-

25. Waar heeft het voorval plaatsgevonden?

(Bent u meerdere malen slachtoffer geworden van een voorval gaarne
aangeven waar het **laatste** voorval heeft plaatsgevonden)

25.a Uw fiets

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.b Uw bromfiets

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.c Uw motor

- ☐ parkeerterrein instelling
- ☐ elders op het terrein van de instelling
- ☐ buiten het terrein van de instelling

25.d Uw auto

- ☐ parkeerterrein instelling
- ☐ elders op het terrein van de instelling
- ☐ buiten het terrein van de instelling

25.e Diefstal van geld of andere persoonlijke eigendommen

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.f Handtastelijkheden

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.g Geweld

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.h Bedreiging

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

25.i Anders, nl.....

- ☐ afsluitbare fietsenstalling
- ☐ open fietsenstalling
- ☐ elders op het terrein
- ☐ buiten het terrein van de instelling
- ☐ elders, nl.....

26. Ondervond u van dit voorval materiële (financiële) schade?

- ☐ Nee, (u kunt doorgaan naar vraag 28)
- ☐ Ja

27. Kunt u een schatting maken van de materiële schade die u en/of uw verzekering daardoor geleden heeft?

f

28. Ondervond u van dit voorval ook enige vorm van immateriële schade ?

- ☐ Nee (u kunt doorgaan naar vraag 30)
- ☐ Ja

29. Welke vorm(en) van immateriële schade hebt u ondervonden?

(U mag meer dan 1 antwoord geven)

- ☐ angst
- ☐ gevoelens van onveiligheid
- ☐ woede
- ☐ wantrouwen
- ☐ anders, namelijk.....

30. Heeft u de gebeurtenis gemeld?

- ☐ nee
- ☐ ja, melding bij de instelling
- ☐ ja, aangifte bij de politie

Preventie

31. Heeft u het afgelopen jaar maatregelen getroffen - ook al bent u geen slachtoffer geworden - tegen de verschillende vormen van criminaliteit waar u in en rond de instelling mee geconfronteerd zou kunnen worden?

nee, want

(gaarne de voor u belangrijkste reden(en) aangeven (maximaal drie))

- ☐ dit is niet noodzakelijk; er komt weinig tot geen criminaliteit voor
- ☐ ik heb al eerder maatregelen genomen
- ☐ het is onmogelijk om maatregelen te treffen
- ☐ maatregelen hebben geen zin
- ☐ ik weet niet welke maatregelen ik moet treffen
- ☐ het is de taak van de instelling om maatregelen te treffen
- ☐ andere reden, namelijk

ja, namelijk

(gaarne de voor u belangrijkste reden(en) aangeven (maximaal drie))

- ☐ veilig opbergen van persoonlijke eigendommen achter slot en grendel
- ☐ maatregelen met betrekking tot de auto (geen waardevolle spullen erin laten, auto-alarm aangebracht)
- ☐ maatregelen met betrekking tot de (brom)fiets (extra slot, in fietsenstalling zetten)
- ☐ waardevolle goederen niet meenemen naar werkplek/daar niets achterlaten
- ☐ maatregelen met betrekking tot komen en gaan in avonduren, late dienst (met anderen gaan, laten ophalen)
- ☐ alert zijn, bewust zijn van gevaren
- ☐ iets bij zich hebben ter bescherming (scherp voorwerk, stuk hout, alarmpieper)
- ☐ zelf meer controleren (onder andere van bezoekers)
- ☐ andere maatregel, namelijk

32. Bent u op de hoogte van de beveiligingsinstructies in de instelling?

- ☐ nee (u kunt vraag 33 overslaan)
- ☐ ja

33. Hoe hebt u daarvan kennis genomen?

- ☐ mondeling, door
- ☐ schriftelijk, door

34. Denkt u dat de afdeling waar u werkt criminaliteitgevoelig is?

- ☐ nee
- ☐ nauwelijks
- ☐ ja, vanwege
(gaarne de voor u belangrijkste reden(en) aangeven (maximaal drie))
 - ☐ het open karakter van de afdeling
 - ☐ de ligging van de afdeling (afgelegen, dichtbij in- of uitgang)
 - ☐ het voorkomen van diefstal en inbraak
 - ☐ niet afsluitbaar zijn van bepaalde ruimtes (garderobes, kasten etc.)
 - ☐ onoverzichtelijkheid van de afdeling
 - ☐ veelheid aan bezoekers en rondlopende mensen
 - ☐ aanwezigheid van waardevolle goederen
 - ☐ aanwezigheid van opiaten, drugs, naalden en medicijnen
 - ☐ geringe personeel/onbemande afdeling
 - ☐ ontbreken van of geringe controle en/of toezicht
 - ☐ gevaar/voorkomen van agressie en bedreiging
 - ☐ overige, namelijk

35. Denkt u dat instelling criminaliteitgevoelig is?

- ☐ nee
- ☐ nauwelijks
- ☐ ja, vanwege
(gaarne de voor u belangrijkste reden(en) aangeven (maximaal drie))
 - ☐ het open karakter van de instelling
 - ☐ de ligging van het gebouw in de omgeving
 - ☐ de indeling van het gebouw (bijvoorbeeld lange, stille, donkere gangen, ingang via brug, ligging van de kelder en de garderobe)
 - ☐ de grootte van het gebouw
 - ☐ de grootte van het terrein
 - ☐ het aantal in- en uitgangen
 - ☐ niet afsluitbaar zijn van bepaalde ruimtes (garderobes, kasten etc.)
 - ☐ onoverzichtelijkheid
 - ☐ veelheid aan bezoekers en rondlopende mensen
 - ☐ onherkenbaarheid van het personeel
 - ☐ aanwezigheid van waardevolle goederen
 - ☐ aanwezigheid van opiaten, drugs, naalden en medicijnen
 - ☐ geringe personeel
 - ☐ ontbreken van of geringe controle en/of toezicht binnen
 - ☐ ontbreken van of geringe controle en/of toezicht buiten
 - ☐ gevaar/voorkomen van agressie en bedreiging
 - ☐ bereikbaarheid, verlichting of onveiligheid van de parkeerplaatsen en/of fietsen-stallingen
 - ☐ anderzins, namelijk

36. Heeft u last van mensen die zonder dat ze daar iets te zoeken hebben over uw afdeling lopen?

- ☐ nee
- ☐ soms
- ☐ regelmatig
- ☐ vaak

37. Wat vindt u dat als eerste criminaliteitsprobleem dient te worden aangepakt?

- ☐ er hoeven geen problemen aangepakt te worden
- ☐ diefstal/beschadiging van (brom)fiets
- ☐ diefstal/beschadiging van motor
- ☐ beschadiging en diefstal van/uit auto
- ☐ diefstal van geld of andere persoonlijke eigendommen
- ☐ handtastelijkheden
- ☐ geweld
- ☐ bedreiging
- ☐ anders, namelijk.....

38. Heeft u suggesties die de veiligheid van mensen en eigendommen in het ziekenhuis kunnen verhogen? (u mag meer dan 1 antwoord geven)

- ☐ afsluitbaar maken van afdelingen
- ☐ afsluitbare opbergmogelijkheden/kleedruimtes
- ☐ camerabewaking
- ☐ meer bewaking
- ☐ langer toezicht vanuit de receptie
- ☐ controle van bezoekers
- ☐ afspraken maken met collega's
- ☐ duidelijke instructies en voorlichting
- ☐ naamplaatje voor medewerkers (met foto)
- ☐ toegangscontrole (pasjessysteem)
- ☐ meer verlichting
- ☐ anders, namelijk

Bedankt voor uw medewerking aan deze enquête. Als u nog vragen hebt, kunt u deze op de volgende bladzijde noteren.

Bijlage 5

Vragenlijst preventiewiel en security audit

VRAGENLIJST PREVENTIEWIEL EN SECURITY AUDIT

67

Deze lijst met vragen is opgesteld aan de hand van het 'Preventiewiel'. De vragenlijst kan mondeling afgenomen worden bij functionarissen die op de hoogte zijn van de beveiligingsplannen en de beveiligingssituatie in een instelling. De informatie die de vragenlijst oplevert, dient aangevuld te worden met geconstateerde feiten en geregistreerde meningen tijdens een observatie-onderzoek.

De lijst begint met een aantal vragen naar de aard en omvang van de criminaliteit binnen de instelling.

Aansluitend komende de volgende onderwerpen aan de orde:

- . Is er een beleid ten aanzien van beveiliging?
- . Hoe is de preventie georganiseerd?
- . Welke regelingen en procedures zijn vastgelegd?
- . Welke voorzieningen zijn er getroffen, zoals
 - . bouwkundige voorzieningen
 - . elektronische voorzieningen
 - . overige voorzieningen?
- . Wat is gedaan aan deskundigheidsbevordering?
- . Hoe is de preventiehouding van het personeel?

In het gesprek kan de volgorde, afhankelijk van de gesprekspartner gewijzigd worden, dan wel kan voor een vrijere interviewmethode gekozen worden.

De vragenlijst is ook als een checklist achteraf te gebruiken.

Inventarisatie criminaliteit

- 1.1. Overzicht van de aard en de omvang van incidenten waarmee uw instelling het afgelopen jaar is geconfronteerd
- 1.2. Hebben er afgelopen jaren ernstige incidenten plaatsgevonden?
- 1.3. Hoe is daarop gereageerd?
- 1.4. Kunt u een schatting geven van de totale schade die de instelling het afgelopen jaar geleden heeft?
- 1.5. Kunt u informatie geven over mogelijke immateriële schade (onrust, angst en dergelijke)
- 1.6. Hebt u een duidelijk beeld van de daders bij de belangrijkste incidenten?
- 1.7. Waar (binnen-buiten), wanneer (dag-nacht) en bij wie zijn eventuele angstgevoelens het sterkst?
- 1.8. Wat zijn naar uw mening de zwakste punten (hoog criminaliteitsniveau en weinig preventievoorzieningen) in uw instelling?
- 1.9. Welke veiligheidsproblemen, waar de instelling mee kampt, zouden naar uw mening met prioriteit aangepakt dienen te worden?
- 1.10. Welke beveiligingsmaatregelen zouden, in het kader van criminaliteitsbestrijding, naar uw mening, als eerste uitgevoerd dienen te worden? Waarom juist die?
- 1.11. Hoe worden slachtoffers van criminaliteit opgevangen? Bestaan daarover afspraken? Kunt u voorbeelden geven?

Het Preventiebeleid

Hieronder volgen enkele vragen die bedoeld zijn om na te gaan of binnen de instelling een duidelijke visie op beveiliging bestaat en of men die heeft vertaald in goede plannen waarmee criminaliteitsrisico's effectief bestreden kunnen worden.

- 2.1 Is er een beveiligingsplan op papier? Of een plan over brandpreventie en/of ontruiming bij calamiteiten?
- 2.2 Hebt u de indruk dat er bij de directie van de instelling een duidelijk beeld bestaat over de omvang en de aard van de criminaliteit? Kunt u uw antwoord toelichten?
- 2.3 Is er bij de top belangstelling voor beveiliging en waardoor wordt die belangstelling gevoed (cijfers, angstgevoelens, incidenten, etcetera).
- 2.4 Als er de afgelopen jaren belangrijke investeringen op het terrein van de beveiliging zijn gedaan, lag daar een duidelijk beleidsplan aan ten grondslag?
- 2.5 Bestaan er nu investeringsplannen voor het treffen van met elkaar samenhangende beveiligingsmaatregelen?
- 2.6 Zijn er al gelden vrijgemaakt/bestemd voor dit doel?
- 2.7 Zijn er voor beveiliging alleen voor dit jaar of voor meerdere jaren gelden beschikbaar gesteld?

De organisatie

We willen graag inzicht hebben in de manier waarop de beveiliging is georganiseerd. Zijn er specialisten voor aangesteld, wat is hun plaats in de organisatie. De gedachte hierachter is, dat een goede beveiligingsorganisatie ook waarborgen biedt voor een effectief beveiligingsbeleid.

70

- 3.1 Wie houden zich binnen de instelling met beveiliging bezig?
- 3.2 Wie is de beleidsverantwoordelijke binnen de directie of het management-team?
- 3.3 Zijn er medewerkers van bijvoorbeeld de technische, de civiele of de portiersdienst, die taken in het kader van de beveiliging uitvoeren?
- 3.4 Welke taken voeren die uit?
- 3.5 Staan die taken duidelijk op papier?
- 3.6 Hebben ze enkel beveiligingstaken of ook andere?
- 3.7 Wat is hun formele plaats in de organisatie?
Wie is hun directe verantwoordelijke?
- 3.8 Zijn hun bevoegdheden helder, bekend en geaccepteerd door een ieder?
- 3.9 Welke opleiding(en) hebben ze genoten?
- 3.10 In welke overlegverbanden komen beveiligingszaken aan de orde?
- 3.11 Zijn de beveiligingsmensen, hun taken en bevoegdheden bekend in de instelling?
- 3.12 Wordt gebruik gemaakt van beveiligingsmensen van commerciële beveiligingsorganisaties?
- 3.13 Vervullen politiemensen nog bepaalde vaste taken in het kader van de beveiliging?
- 3.14 Door wie wordt toezicht uitgeoefend op beveiligingsmaatregelen en beveiligingsmensen?

Procedures en regelingen

Een organisatie kan soepel lopen als er regelingen, werkafspraken en vaste manieren van werken zijn. Vaste procedures voorkomen veelvuldig overleg en onzekerheid over hoe in bepaalde situatie gehandeld moet worden. Ze vormen dus een noodzakelijke aanvulling op de organisatiestructuur.

We hebben een aantal vragen geformuleerd om na te gaan of er ook ten aanzien van de beveiliging dergelijke vaste routines bestaan.

- 4.1 Staan er regelingen op papier over
 - a. alarmering?
 - b. melding van incidenten (kleine criminaliteit)?
 - c. sleutelbeheer?
 - d. dienstrooster bewakingspersoneel?
 - e. inspectierondes?
 - f. bewaking computerbestanden, databeheer, dossiers?
 - g. toegangscontrole, legitimatie?
 - h. anders, namelijk?
- 4.2 Hoe werken die regelingen?
- 4.3 Hoe wordt de handhaving van die regelingen gecontroleerd?
- 4.4 Vindt er systematische registratie van diefstal etcetera plaats?
- 4.5 Worden hierbij vaste incidentmeldingsformulieren gebruikt?
- 4.6 Bij wie is het sleutelbeheer ondergebracht? Hoe is dat geregeld?
- 4.7 Zijn er afspraken over vaste controle-rondes? Hoe wordt dat uitgevoerd?
- 4.8 Zijn er duidelijke werkafspraken met de politie?
- 4.9 Zijn er zorgvuldige procedures voor slachtoffers van incidenten? Zijn er verschillen wanneer het gaat om patiënten/kliënten, medewerkers, bezoekers van patiënten/kliënten?

Technische voorzieningen

Als 'paradepaardjes' van de beveiliging worden doorgaans de technische maatregelen beschouwd. We willen inzicht krijgen in de omvang en de kwaliteit van de voorzieningen die getroffen zijn. Achtereenvolgens stellen we vragen over de gerealiseerde bouwkundige maatregelen, de toegepaste elektronische systemen en eventuele andere, meer technische voorzieningen.

A. Bouwkundige voorzieningen

72

- 5.1 Is er bij de bouw (in het programma van eisen) rekening gehouden met beveiligingsaspecten?
- 5.2 Worden er bepaalde delen van de gebouwen afgesloten als er geen werkzaamheden plaatsvinden (compartimentering, zonering)?
- 5.3 Hoe waardeert u de beveiliging van het terrein?

meer specifiek:
 - a. de omheining (toegankelijk, sterk)?
 - b. de wegen (veilig)?
 - c. de groenvoorziening (doorzichtig-camouflerend)?
 - d. het materiaalgebruik (van gevels en dergelijke)?
 - e. de fietsenstalling (veilig benaderbaar, afgesloten)?
 - f. de parkeervoorziening (bewaakt)?
(denk hierbij aan aspecten als:
 - afstand tot het hoofdgebouw
 - in/uit het zicht
 - verlichting
 - toegankelijk voor derden
 - sloten/afsluitbaarheid
 - hoe bewaakt (slagbomen, bewakers, bewegwijzering)
- 5.4 In hoeverre is in het gebouw aandacht aan beveiliging geschonken bij:
 - a. aantal in- en uitgangen?
 - b. mogelijke vluchtwegen?
 - c. routing/bewegwijzering?
 - d. zichtbelemmerende obstakels?
 - e. deuren en ramen (aantal, toegankelijkheid)?
 - f. hang- en sluitwerk?
 - g. inbraakwerende ruiten (portiersloge bijvoorbeeld)?
- 5.5 Waar zijn de garderobes (centraal/decentraal)?
Hoe zijn die beveiligd?
- 5.6 Welke voorzieningen zijn er voor de waardebergingen van eigendommen van patinten/kliënten en hoe functioneren die?
- 5.7 Welke voorzieningen zijn er voor de waardebergingen van eigendommen van personeel en hoe functioneren die?
- 5.8 Waar zijn medicijnkasten? Welke soort? Hoe beveiligd?

B. Elektronische voorzieningen

6.1 Waar is in verband met beveiliging elektronica aangebracht?

6.2 Welke systemen zijn er? Waar zijn die geplaatst?

Denk aan:

- a. gesloten TV-circuit
- b. inbraakdetectie op deuren
- c. communicatiesystemen (telefoons, piepers en dergelijke)
- d. elektronische slotensystemen
- e. toegangscontrole-systeem.

6.3 Wat is de kwaliteit van deze apparatuur en hoe is zij aangebracht?

6.4 Wat waren de aanleidingen om juist die elektronica op deze plaatsen aan te brengen?

6.5 Op welke manier hebt u een keuze kunnen maken uit het grote aanbod op dit terrein?

6.6 Kunt u een indicatie geven over de investeringskosten van de elektronica die het afgelopen jaar is geïnstalleerd?

6.7 Hoe waardeert u de functionaliteit van deze systemen in het kader van de preventie?

6.8 Is er een Key-card systeem in gebruik? Wordt dit overwogen? Welk systeem heeft de voorkeur? Waarom?

C. Overige voorzieningen

7.1 Zijn er andere voorzieningen die u getroffen heeft om mensen en goederen in uw instelling te beveiligen?

Denk aan:

- a. Markering van eigendommen/inventaris
- b. Badges-systeem/pasjes-systeem
- c. Sleutelsysteem
- d. routing, bewegwijzering
- e. verlichting.

7.2 Hoe is de functionaliteit van deze systemen in de praktijk?

Deskundigheidsbevordering

Een beveiligingssysteem is afhankelijk van de mate waarin management en medewerkers weten wat ze moeten doen. Deskundigheid van het beveiligingspersoneel en goede informatie over de risico's en gedragsregels die vastgesteld zijn, is daarvoor onontbeerlijk. Met enkele vragen willen we meten in hoeverre de condities daarvoor aanwezig zijn.

74

- 8.1 Welke medewerkers hebben gespecialiseerde opleidingen of trainingen op beveiligingsgebied gevolgd?
- 8.2 Zijn er op dit moment medewerkers in opleiding, of zijn er opleidingen gepland?
- 8.3 Nemen beveiligingsmensen deel aan 'netwerken' waarin met collega's over het vak gesproken wordt? Welke zijn dat?
- 8.4 In hoeverre is de directie vertrouwd met inzichten over en kennis van de beveiliging?
- 8.5 Hoe is/wordt het personeel geïnformeerd over
 - a. criminaliteitsincidenten
 - b. criminaliteitsrisico's
 - c. vastgestelde procedures en maatregelen
(Gebeurt dat regelmatig? Door wie? Wat is het effect?)
- 8.6 Waar denkt u dat de belangrijkste hiaten zitten?
 - a. in de deskundigheid bij beveiligingsmensen?
 - b. de informatie bij het management?
 - c. de informatie bij het personeel?

Preventiehouding

Alertheid van management en medewerkers waar het de beveiliging betreft is een vereiste om ervoor te zorgen dat de beveiligingsorganisatie doeltreffend blijft werken en de technische voorzieningen ook daadwerkelijk het beoogde effect hebben.

Veel is dus afhankelijk van de houding ten opzichte van preventie bij management en medewerkers van een instelling.

Daarover tenslotte enkele vragen.

- 9.1 Is de leiding van deze instelling zorgvuldig in de naleving van de procedures en regelingen die gemaakt zijn in het kader van de beveiliging?
- 9.2 Zijn de beveiligingsmensen in staat om medewerkers erop te attenderen wanneer de regels niet nageleefd worden?
- 9.3 Bestaat er bij medewerkers in het algemeen een duidelijk besef van de criminaliteitsrisico's?
- 9.4 Voelt men zich veilig?
- 9.5 Hoe worden deze angstgevoelens naar voren gebracht en hoe reageert de leiding daarop?
- 9.6 Zijn medewerkers zorgvuldig in de naleving van de regels?
- 9.7 Laten de medewerkers zich gemakkelijk corrigeren?
- 9.8 Corrigeren medewerkers elkaar gemakkelijk wanneer ze onderling een bepaalde laksheid constateren?
- 9.9 Is men gemotiveerd om meer aan preventie te doen en aan wat voor maatregelen denkt men dan bij voorkeur?
- 9.10 Worden beveiligingsinstallaties en -procedures regelmatig getest?
- 9.11 Worden slachtoffers goed opgevangen?

75

Zijn er tenslotte nog andere punten die u wilt noemen?

Bedankt voor uw medewerking?

Bijlage 6

Voorbeeld incidentmeldingformulier

PROCES-VERBAAL VAN AANGIFTE

78

Dienst : Regiopolitie	
Datum aangifte :	
Rapportagenummer :	
Verbalisant :	
Naam aangever/gemachtigde:	
Voorna(a)m(en) :	Geboorteplaats:
Geboortedatum :	
Woonadres :	Woonplaats:
Postcode :	Werk:
Telefoon (privé) :	
Naam eigenaar/benadeelde:	
Persoon:	
Rechtsvorm :	
(Achter)naam :	
Voorna(a)m(en) :	Geboorteplaats:
Geboortedatum :	
Adres :	Woonplaats:
Postcode :	Werk:
Telefoon (privé) :	
Datum delict : dag maand uur mn en dag maand uur mn	
Op/tussen :	
Pleegplaats :	Gemeente:
Straatnaam :	huisnummer:
Ontvreemd/schade: Zie omschrijving goederen en/of schade	
Verklaring aangever/gemachtigde: Zie verklaring aangever.	
Werkwijze :	
Opsporingsmaatregelen	
HKD-onderzoek :	Resultaat:
Foto's getoond :	
Naam/fotonr.verdachte(n):	Resultaat:
Techn.sporen onderzoek :	
Waarvan door mij op ambtseed/-belofte is opgemaakt, dit proces-verbaal, gesloten en ondertekend te:	
op:	
(handtekening verbalisant)	

PROCES-VERBAAL

79

OMSCHRIJVING GOEDEREN EN/OF SCHADE
(indien ruimte te klein volgend blad gebruiken)

PROCES-VERBAAL

80

Naam aangever :		
Adres :		
O (04)	boeken/drukwerk/documenten	Bijzondere kenmerken:
Waar vandaan weggenomen:		
O (06)	brandkast/kuis/geldkist	Merk:
	Bijzondere kenmerken:	Type:
Waar vandaan weggenomen:		
O (16)	film/fotomateriaal/optiek	Merk:
	Bijzondere kenmerken:	Type:
Waar vandaan weggenomen:		
O (17)	geld	:
Waar vandaan weggenomen:		
O (18)	geluid- en beeldapparatuur/ drager	Merk:
	Bijzonder kenmerken:	Type:
Waar vandaan weggenomen:		
O (19)	gereedschap	Merk:
	Bijzondere kenmerken:	Type:
Waar vandaan weggenomen:		
O (20)	horloges/klokken	Merk:
	Bijzondere kenmerken:	Type:
Waar vandaan weggenomen:		
O (21)	huishoudelijke artikelen/ apparatuur	:
	Bijzondere kenmerken:	Merk:
		Type:
Waar vandaan weggenomen:		
O (22)	identiteitspapieren	O paspoortnummer:
		O rijbewijs nummer:
		O anders, namelijk:
Waar vandaan weggenomen:		

O (23)	juwelen/sieraden	☐ ring ☐ armband ☐ ketting ☐ broche ☐ anders, namelijk:	Kenmerken:
Waar vandaan weggenomen:			
O (24)	kantoorartikelen	:	Waar vandaan weggenomen:
O (26)	kentekenbewijzen e.d.	:	Waar vandaan weggenomen:
O (27)	kleding/textiel/schoeisel	:	Waar vandaan weggenomen:
O (28)	kunst	:	Bijzondere kenmerken: Waar vandaan weggenomen:
O (29)	medicamenten/narcotica	:	Waar vandaan weggenomen:
O (30)	meubilair/stoffering e.d.	:	Bijzondere kenmerken: Waar vandaan weggenomen:
O (36)	portemonnaie/portefeuille	Merk: Inhoud: Bijzondere kenmerken:	Kleur: Waar vandaan weggenomen:
O (38)	sleutels	:	Bijzondere kenmerken: Waar vandaan weggenomen:

O (39) speelgoed/sportartikelen :		Merk:		Bijzondere kenmerken:		Waar vandaan weggenomen:	
O (42) vervoermiddel		☐ auto ☐ motor ☐ bromfiets ☐ fiets ☐ anders, namelijk:					
Merk:		Type:		Kleur:		Kenteken:	
		Bijzondere kenmerken:					
		Waar vandaan weggenomen:					
O (44) voeding/genotmiddelen :		Waar vandaan weggenomen:					
O (45) waardepapieren		☐ betaalkaarten ☐ cheques ☐ creditcards ☐ anders, namelijk: Waar vandaan weggenomen:					
O (47) zak/tas/koffer :		Merk:		Type:		Kleur:	
		Waar vandaan weggenomen:					
O (35) overige :		Waar vandaan weggenomen:					
Ruimte voor specificatie: (indien nodig bijlage gebruiken)							

Bijlage 7

Voorbeeld communicatieplan

1. Introductie Beveiligingscommissies	
Bijeenkomst Beveiligingscommissies	
Doelgroep	Leden van de beveiligingscommissies
Medium	Een gezamenlijke bijeenkomst van de beveiligingscommissies
Doel	Informeren over de stand van zaken van het project, en instructie over taak en functie van beveiligingscommissies in het project
Inhoud	- Kennismaking - Ontwikkelingen tot nu toe - Inleiding integrale beveiliging/integrale aanpak van beveiliging - Uitleg over gebruikte methoden: incidentenregistratie, personeelsenquete, kleurenmethode en security-audits - Taken en verantwoordelijkheden van de commissies - Formuleren van beveiligingsbeleid - Invoering van dit beleid - Samenwerking met de politie - Fotograferen van de commissies ten behoeve van de schriftelijke introductie
Datum	
Actie door	

2. Introductie Beveiligingsproject

Schriftelijke introductie beveiligingsproject en beveiligingscommissies

Doelgroep	Personeel van de instellingen.
Medium	Een artikel in het personeelsblad en/of circulaire.
Doel	Personeel informeren over de start van het project en de functie van de beveiligingscommissie.
Inhoud	- Noodzaak van een aanpak van de beveiliging. - De doelstellingen. - De aanpak en duur van het project. - Samenstelling van de beveiligingscommissie. - Wat doet de commissie en hoe zijn de leden van de commissie te bereiken?
Datum	Na de formele opdracht tot het houden van een project.
Actie door	Projectcoördinator: aanleveren van standaardteksten. Interne projectcoördinator: aanvullen van specifieke gegevens en zorgdragen voor publicatie.

Mondelinge introductie beveiligingsproject en beveiligingscommissies

Doelgroep	Het management.
Medium	Toelichting geven in het management-overleg door lid van de beveiligingscommissie.
Doel	Informeren van management en daarmee verhogen van draagvlak voor aanpak van beveiliging.
Inhoud	- Noodzaak van een aanpak van de beveiliging. - De doelstellingen. - De aanpak en duur van het project. - Samenstelling van de beveiligingscommissie. - Wat doet de commissie en hoe zijn de leden van de commissie te bereiken?
Datum	Zo spoedig mogelijk na formele opdracht tot het houden van een project.
Actie door	Interne projectcoördinator.

3. Voortgang Beveiligingsproject	
Informatiebijeenkomst	
Doelgroep	Het management.
Medium	Informatiebijeenkomst in het managementteam en/of overleg tussen interne projectcoördinator en verantwoordelijk directeur.
Doel	Informeren van directie en management over de voortgang van het project.
Inhoud	Afhankelijk van het stadium waarin het project zich bevindt.
Datum	Bij afronding van elke fase.
Actie door	Projectcoördinator. Interne projectcoördinator en/of lid van het managementteam dat zitting heeft in de interne beveiligingscommissie.
Schriftelijke rapportage	
Doelgroep	Het personeel van de instelling.
Medium	Een artikel in het personeelsblad en/of circulaire.
Doel	Informeren van de medewerkers over de voortgang van het project.
Inhoud	Afhankelijk van het stadium waarin het project zich bevindt.
Datum	Na afronding van elke fase.
Actie door	Projectcoördinator en/of interne projectcoördinator.

4. Introductie Methoden	
Schriftelijke instructie en/of mondelinge informatie	
Doelgroep	Personeel van de instelling.
Medium	Personeelsblad en/of circulaire en/of mondelinge toelichting.
Doel	Methoden introduceren bij de medewerkers.
Inhoud	Introductie personeelsenquete. Doel van de personeelsenquete · belang van invullen van de personeelsenquete · datum waarop de enquête verzonden wordt. Introductie incidentenregistratie. Doel van de incidentenregistratie · belang van het doen van aangifte · uitleg van procedure incidentenregistratie. Introductie kleurenmethode. Doel van de kleurenmethode · wat is de kleurenmethode? · belang van de kleurenmethode · wanneer wordt de kleurenmethode uitgevoerd · welke medewerking wordt verlangd? Introductie security-audit. Doel van de security-audit · wat is een security-audit? · wanneer wordt de security-audit gehouden · wat wordt van iedereen verwacht
Datum	twee weken voorafgaand aan de toepassing van de onderzoeksmethode.
Actie door	Projectcoördinator: ondersteuning bieden. Interne projectcoördinator. Leden beveiligingscommissie.

5. Eindresultaten Onderzoeksmethoden

Informatiebijeenkomst en mondeling overleg met de voor beveiliging verantwoordelijke directeur

Doelgroep	Het management.
Medium	Informatiebijeenkomst in het managementteam en overleg tussen interne projectcoördinator en verantwoordelijk directeur.
Doel	Informeren van directie en management over de uitkomsten van de onderzoeksmethoden.
Inhoud	Resultaten project en aanbevelingen.
Datum	Na afronding van de rapportage.
Actie door	Projectcoördinator. Interne projectcoördinator en/of lid van het managementteam dat zitting heeft in de interne beveiligingscommissie.

Informatiebijeenkomst

Doelgroep	Het personeel van de instelling.
Medium	Informatiebijeenkomst per instelling.
Doel	Personeel op de hoogte brengen van de resultaten van de personeelsenquete, de kleurenmethode, de security-audit en de geregistreerde gegevens.
Inhoud	Presentatie resultaten project en aanbevelingen.
Datum	Na de rapportage van de uitkomsten.
Actie door	Projectcoördinator (ondersteuning bieden). Interne projectcoördinator. Leden beveiligingscommissie.

6. Persvoorlichting

Doelgroep	Landelijke en regionale pers.
Medium	Persbericht en persconferentie.
Doel	Bekendheid geven aan de beveiligingsaanpak binnen de instellingen.
Inhoud	Resultaten project.
Datum	Na beëindigen project en vaststelling van het beveiligingsbeleidsplan.
Actie door	Externe projectcoördinator.

Bijlage 8

Overzicht van Vetron beveiligingsinstituten- en trainingen

Overzicht van bij de Vetron aangesloten beveiligingsinstituten en -trainingen

Naam training:	Bestemd voor:	Opleidingsinstituut:	Duur:
Security & audit Local Area Networks met Novell	Hoofden van gebruikersafdelingen Systeem- en netwerkbeheerders Beveiligingsfunctionarissen, en EDP-auditors	KPMG Klynveld Management Trainingen	2 dagen
Security & audit UNIX en TCP/IP	Hoofden van administratieve afdelingen Systeem- en applicatiebeheerders Beveiligingsfunctionarissen, en EDP-auditors	KPMG Klynveld Management Trainingen	2 dagen
Milieu-auditing	Functionarissen die belast zijn of worden met de uitvoering of begeleiding van milieu-audits in de eigen organisatie	KPMG Klynveld Management Trainingen	3 dagen
Beveiliging en Riskmanagement	Facility-managers, beveiligings- functionarissen, hoofden computercentra.	Bureau Zuidema	2 dagen

Voor verdere informatie kunt u zich wenden tot:
Vetron
p/a Wissenraet, secretariaats- en bestuurservice
Postbus 84200
2508 AE 's-Gravenhage
Van Stolkweg 34
2585 JR 's-Gravenhage
Telefoon: 070 - 3505995
Fax: 070 - 3544067

Bijlage 9

Aandachtspunten bij de aanpak van agressie en geweld

9.1 Inleiding

In de Arbo-wet worden agressie en seksuele intimidatie alsmede de gevolgen van deze vormen van criminaliteit specifiek genoemd als risico's waartegen de werkgever de werknemer zoveel mogelijk dient te beschermen. Dit betekent dat de werkgever een taak heeft op het gebied van zowel de preventie van agressie en seksuele intimidatie als op het gebied van de opvang en nazorg van getroffen werknemers. Om aan de eisen van de wet te kunnen voldoen zal binnen de zorginstelling eerst de agressie-problematiek in kaart gebracht moeten worden en zal meer bekend moeten worden over de aard en omvang van agressie in de instelling. Ook de specifieke oorzaken van agressie zullen onderzocht moeten worden alvorens tot maatregelen en verbeteringen overgegaan kan worden.

92

9.2 Aard en omvang van agressie en geweld

Onder agressie en geweld wordt verstaan:

- fysiek geweld: het (met of zonder wapen) toebrengen van lichamelijk letsel;
- verbaal geweld: uitschelden, bedreigen, vernederen, ruzie;
- intimidatie: iemand bedreigen om iets gedaan te krijgen;
- achtervolgen en lastig vallen;
- seksuele intimidatie;
- discriminatie: negatieve opmerkingen in verband met iemands geslacht, huidskleur of andere kenmerken.

Helaas houden slechts weinig zorginstellingen een goede incidentenregistratie bij, waardoor betrouwbaar cijfermateriaal over de aard en omvang van agressie in zorginstellingen ontbreekt. Uit Brits onderzoek blijkt overigens wel dat de omvang van agressie per type zorginstelling en per afdeling varieert. Schema 1 geeft een overzicht.

Schema 1: Agressie-top 5 zorginstellingen in Engeland

Zorginstelling	% van alle werknemers dat per jaar één of meerdere keren slachtoffer wordt van agressie
1 Psychiatrische ziekenhuizen/inrichtingen	27
2 Verpleegafdelingen van algemene ziekenhuizen	26
3 Geriatrische zorginstellingen	21
4 Spoed eisende hulp-post van algemene ziekenhuizen	20
5 Algemene ziekenhuizen (gemiddelde van alle afdelingen)	9

Bron: Health Services Advisory Committee 1986.

In psychiatrische ziekenhuizen wordt door het management agressie tegen het personeel meer als probleem onderkend dan in algemene ziekenhuizen, terwijl daar de agressie-problemen op bepaalde afdelingen eveneens omvangrijk zijn. Behalve het slachtoffer zelf, zijn overigens ook de getuigen en degenen die het slachtoffer willen helpen, te beschouwen als getroffenen. Ook zij beleven het incident mee en zullen de ervaring moeten verwerken. Zo kunnen andere patiënten er bijvoorbeeld ook last van hebben als er op hun afdeling ruzie ontstaat tussen een patiënt en een verpleger, of kunnen psychiatrisch verpleegkundigen zich extra onveilig gaan voelen als een collega uit hun team door een patiënt is mishandeld.

9.3 Oorzaken van agressie

93

Mensen die agressief of gewelddadig zijn, kunnen daarvoor verschillende redenen hebben. Op grond van deze motieven kan er onderscheid gemaakt worden tussen vier vormen van agressie:

- * instrumentele agressie: een medewerker onder druk zetten om een bepaald doel te bereiken (b.v. om een gunstige beslissing af te dwingen, om pijn te vermijden of om geld te krijgen (overval));
- * expressieve agressie: het uiten van een algemeen gevoel van onvrede, machteloosheid of irritatie ten aanzien van een situatie, medewerker, locatie of instelling;
- * agressie tussen werknemers en klanten (patiënten, bezoekers) als gevolg van concrete conflicten of belangentegenstellingen.
- * willekeurige agressie: agressie waarbij de instelling fungeert als een soort bliksemafleider waarop mensen hun elders opgedane agressieve gevoelens kunnen afreageren.

In ziekenhuizen blijken verpleegkundigen, en dan met name de leerling-verpleegkundigen, het meest met incidenten geconfronteerd te worden. Dit is niet zo verwonderlijk aangezien verpleegkundigen ook het meest frequent contact hebben met patiënten en hun bezoekers.

Ook de aard van de werkzaamheden van verpleegkundigen kan agressie oproepen. Verpleegkundigen voeren handelingen uit die pijnlijk, beangstigend of frustrerend kunnen zijn voor patiënten. Wanneer de dienstverlening dan niet optimaal is (voorlichting en begeleiding) kunnen deze handelingen agressief gedrag tot gevolg hebben.

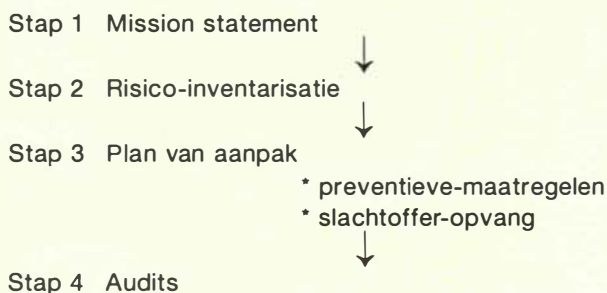
Door de overheid wordt al jaren een fors bezuinigingsbeleid doorgevoerd. Zorginstellingen worden geacht met steeds minder financiële steun van de overheid toch dezelfde diensten te blijven verlenen. Doordat de instellingen met name op personeelskosten bezuinigen, moet met steeds minder mensen hetzelfde werk gedaan worden. Dit gaat onherroepelijk ten koste van de dienstverlening: langere wachttijden, minder plaats voor patiënten, die na een ingreep zo snel mogelijk weer naar huis worden gestuurd en een lagere prioriteit voor de sociale kant van de verpleging, want voor een praatje is nauwelijks tijd. Het bezuinigingsbeleid van de overheid kan daarom ook gezien worden als een factor die kan bijdragen tot agressie.

9.4 Aanpak van agressie in Arbo-perspectief

Er bestaat geen trainingsonderdeel binnen de opleiding om de leerlingverpleegkundigen voor te bereiden op agressie van patiënten en bezoekers. Het leren omgaan met agressie en geweld gebeurt daarom bijna altijd in de praktijk en dit pakt niet altijd goed uit. De negatieve ervaringen blijken vaak niet goed bespreekbaar te zijn, waardoor getroffenen niet opgevangen worden en men niet van elkaars ervaringen kan

leren. Aldus stapelen de ervaringen met criminaliteit en agressie zich langzaam maar zeker op. Deze praktijk staat haaks op de door de wetgever gewenste situatie. In de Arbo-wet is namelijk een bepaling opgenomen die de werkgever verplicht tot het geven van voorlichting en onderricht in verband met veiligheid, gezondheid en welzijn van de werknemer, met name aan jeugdige werknemers. De huidige gang van zaken is dus niet alleen onbevredigend, maar wettelijk gezien ook onjuist. De werkgever is op grond van de Arbo-wet verplicht zorg te dragen voor de veiligheid, gezondheid en het welzijn van de werknemer in verband met arbeid. Bij het Arbo-beleid hoort ook het creëren van veilige werkmethoden en het aanpakken bij de bron van mogelijke gevaren. Om aan de verplichtingen van de Arbo-wet te kunnen voldoen, zal een plan van aanpak noodzakelijk zijn. Schema 2 geeft een overzicht.

Schema 2: Aanpak van agressie volgens de Arbo-systematiek



Stap 1 Mission statement

Agressie en geweld kunnen alleen structureel aangepakt worden als het probleem erkend wordt. De erkenning van het probleem ontbreekt echter nogal eens: managers en leidingsgevenden, maar in veel gevallen ook de medewerkers zelf, hebben vaak een zeer tolerante houding tegenover geweld en agressie van klanten jegens medewerkers ("dat hoort er nu eenmaal bij"). Dergelijke bedrijfsculturen verdienen een kritische revisie. In sommige organisaties kan het probleem daarom pas echt structureel aangepakt worden nadat er een cultuuromslag heeft plaatsgevonden. Hierbij speelt de leiding een cruciale rol.

Het is belangrijk dat het management door middel van een intentieverklaring of mission statement expliciet aangeeft dat het agressie en geweld serieus neemt en dat het bereid is om het probleem structureel aan te pakken.

Stap 2 Risico-inventarisatie

Alvorens het probleem aan te kunnen pakken, dient allereerst de bestaande situatie in kaart gebracht te worden. Beschreven moet worden waar de risico's van agressie en geweld zich voordoen en wat er verbeterd kan worden op het gebied van preventie en nazorg. De inventarisatie zal zich zowel op de 'technische' kant moeten richten, waarbij vooral de inrichting van het gebouw aan de orde zal komen, alsmede op de 'sociale' kant: hoe kan het werk zo ingericht worden dat er minder kans is op agressie en geweld, en als er toch incidenten plaatsvinden hoe vangt men die dan op.

Aangezien agressie en geweld zich op de werkvloer manifesteert, is het van groot belang dat de werknemers vanaf het begin betrokken worden - en ook betrokken blijven - bij het aanpakken van dit probleem. Idealiter wordt de aanpak langs twee wegen ontwikkeld: top down én bottom up. Bottom up betekent dat aan de werknemers

wordt gevraagd welke (risico-)factoren een rol spelen bij het ontstaan van agressie in concrete situaties. Deze informatie, die gesystematiseerd kan worden door het invoeren van een registratie van agressieve incidenten, is van onschatbare waarde bij het bepalen van de risico's en het bedenken van maatregelen. Andersom (top-down) beschikt het management over kennis van en overzicht over de totale organisatie, waardoor minder zichtbare achterliggende oorzaken van de problematiek, zoals aspecten van de bedrijfsvoering en de bedrijfscultuur, achterhaald kunnen worden. Door het samenbrengen van concrete 'werkvloerkennis' en de wat abstractere inzichten op managementniveau ontstaat een volledig en diepgaand beeld van de problematiek.

Stap 3 Maatregelen

95

Na het in kaart brengen van de aard en omvang van de problematiek kan de bestaande situatie vergeleken worden met de gewenste situatie. Uit die vergelijking zullen knelpunten naar voren komen, waarin prioriteiten gesteld moeten worden. Immers, niet alle knelpunten zullen even dringend zijn en even snel op te lossen. Sommige verbeteringen en oplossingen kunnen eenvoudig en snel doorgevoerd worden, anderen zullen gefaseerd in meerjarenplannen aan bod kunnen komen.

Wanneer de prioriteiten zijn vastgesteld kunnen bijpassende maatregelen gezocht worden.

Een goede aanpak rust op twee pijlers, te weten:

- 1 Een preventieve aanpak gericht op de verhoging van de veiligheid van werknemers. Dit aspect wordt ook wel aangeduid met de term 'veiligheidsbeleid'.
- 2 Een curatieve aanpak gericht op het verzachten van de gevolgen van agressie en geweld bij de slachtoffers (het opvangbeleid).

Het weglaten van één van deze twee pijlers is ofwel verspilling van geld en moeite (als er alleen aandacht is voor het opvangen van de slachtoffers terwijl er niets aan preventie wordt gedaan) ofwel volkomen ongeloofwaardig (als men de slachtoffers in de kou laat staan).

Preventieve maatregelen

Op het preventieve vlak valt te denken aan de volgende maatregelen.

- 1 Voorlichting en draagvlakvergroting
Allereerst moeten de medewerkers zich door middel van voorlichting bewust worden van de mate waarin agressie voorkomt en hoe collega's daarmee omgaan. Door voorlichtingsdagen kan ook een draagvlakvergroting plaatsvinden voor het veiligheidsbeleid.
- 2 Technische voorzieningen
Ter voorkoming van agressie en intimidatie kunnen maatregelen genomen worden in de sfeer van technopreventie. Met behulp van 'hardware' middelen, zoals hangen sluitwerk, alarmknoppen e.d. kan de fysieke werkomgeving veiliger gemaakt worden.
- 3 Ontwikkelen en vastleggen van procedures bijvoorbeeld in de vorm van een draaiboek "Omgaan met agressie"
Behalve techno-preventieve maatregelen zullen ook maatregelen aan de socio-preventiekant genomen moeten worden: hoe kan de werkwijze aangepast worden, opdat er minder agressie en geweld plaats zal vinden. In dit verband kan gedacht worden aan het ontwikkelen van een draaiboek 'hoe om te gaan met agressieve patiënten en bezoekers'. In zo'n draaiboek worden de probleemsituaties omschreven en de procedures en richtlijnen die aangeven hoe de instelling met dit soort situaties omgaat.
- 4 Deskundigheidsbevordering
Medewerkers kunnen leren om adequaat om te gaan met agressie. Er bestaan in

dit kader vele trainingen, met name ontwikkeld in de psychiatrie, op basis van verschillende uitgangspunten.

Mogelijke uitgangspunten zijn:

- de houding van de verpleegkundige ten aanzien van de agressor;
- fysieke beheersing van agressieve patiënten;
- het bespreekbaar maken van agressie binnen het eigen team.

Slachtoffer-opvang

Omdat agressie en geweld niet altijd voorkomen kan worden, zal er ook aan de opvangkant het een en ander moeten gebeuren. De opvang kan op verschillende manieren ingericht worden. Er kan een keuze gemaakt worden voor opvang middels het werkoverleg - het binnen het eigen team bespreekbaar maken van agressie - of voor opvang door speciaal daarvoor aangewezen sleutelpersonen in de organisatie. Ook kan gebruik gemaakt worden van hulpverlenende instanties en andere externe deskundigen.

96

Een overzicht van organisaties die zorginstellingen professionele ondersteuning kunnen bieden bij het opvangen van werknemers die slachtoffer zijn geworden van agressie en (seksueel) geweld op de werkplek en/of kunnen adviseren bij het opzetten van een opvangbeleid op diskette is beperkt aan te vragen bij:

v. Dijk, v. Someren en Partners

Mariotteplein 9

1098 NW Amsterdam

Opvang door teamleden middels het werkoverleg

In dit model is het de bedoeling dat gedurende het werkoverleg de door de teamleden meegemaakte agressie-incidenten en schokkende gebeurtenissen in teamverband besproken kunnen worden. Het verdient dan de voorkeur om deze gesprekken te voeren aan de hand van vaste gespreksprotocollen.

Deze vorm van opvang is gebaseerd op de volgende twee uitgangspunten:

- Medewerkers zijn deskundig op het terrein van agressie.
- Medewerkers verlenen elkaar voor en na agressieve incidenten collegiale steun.

De collegiale steun vormt zowel de primaire als de secundaire preventie. Primair is de preventieve steun: een collega die te hulp schiet als een situatie uit de hand dreigt te lopen. Secundair is de curatieve steun: medewerkers hebben na een agressief incident aandacht en opvang nodig.

Het voeren van zulke teamgesprekken kan geleerd worden middels trainingen. Zo'n training dient bij voorkeur de volgende twee doelstellingen te hebben:

- 1 het reduceren van agressie (en seksuele intimidatie) jegens medewerkers;
- 2 werknemers te immuniseren voor stressreacties tijdens en na agressieve bejegeningen van patiënten.

Onderdelen die tijdens zo'n training aan de orde dienen te komen zijn:

- * het overwinnen van weerstand tegen leren (ervaren);
- * leren bespreken van de eigen ervaringen met agressie op het werk;
- * leren bespreken van de oorzaken en gevolgde aanpak bij de eigen ervaringen met agressie, inclusief normen en waarden en een evaluatie van sterke en zwakke elementen van de aanpak;
- * bespreken van de wijze van registreren van agressieve incidenten alsmede het notuleren tijdens een teamoverleg;
- * brainstormen over verbeteringen in de aanpak van agressie, waaronder veiligheid en opvang.

Uit de ervaringen die opgedaan zijn met zulke teamoverleggen is in de eerste plaats duidelijk geworden dat opvang vooraf moet gaan aan het verbeteren van de veiligheid. Medewerkers moeten het gevoel hebben dat er naar hen geluisterd wordt, alvorens zij zich open en creatief wensen in te zetten voor een aanpak van de opvang en veiligheid in de instelling. Ten tweede is een beleidsmatig kader voor het uitvoeren van zulke opvanggesprekken in het teamoverleg onmisbaar. Hier zal het Arbo-jaarplan een belangrijke rol in spelen, want daarin staat gedefinieerd welke doelen men voor ogen heeft op Arbo-gebied, op welk budget dit berust en in welk tijdsbestek een en ander gerealiseerd dient te worden.

Opvang door speciale sleutelpersonen in de organisatie

Een tweede model dat gehanteerd kan worden, is het aanwijzen van speciale sleutelpersonen in de organisatie die de opvang verzorgen. Deze vorm van opvang na een agressief incident is met name goed toepasbaar wanneer het team veelvuldige veranderingen in samenstelling kent en in organisaties waar bijvoorbeeld door reorganisaties een sterke beoordelingsbeduchtheid heerst. Het is in deze laatste situatie niet eenvoudig om 'te biecht' te gaan bij collega's en teamleider, indien men vermoedt dat de informatie ook op het beoordelingsgesprek naar voren zal komen. Ook het opvangen van slachtoffers van ongewenste intimiteiten of andere zedendelicten gebeurt vaak door speciale sleutelpersonen.

Het is belangrijk dat deze sleutelpersonen goed voor hun taak toegerust zijn en training is in dit verband meestal onmisbaar. In zo'n training leert een sleutelpersoon meestal drie soorten gesprekken te voeren met slachtoffers van agressieve incidenten, aan de hand van vaste gespreksprotocollen. De drie gesprekken hebben ieder hun eigen karakter en worden gevoerd meteen na het incident, een paar dagen daarna en weer enkele weken daarna. Vanuit de informatie die in deze gesprekken naar voren komt kan de opvang beoordeeld worden of er sprake is van verwerking, dan wel of het verstandig is om bijvoorbeeld verdergaande opvang te regelen bij het bedrijfsmaatschappelijk werk.

Ook dit model van opvang dient in het eerder beschreven beleidsmatig kader van de organisatie geplaatst te worden. Bij de medewerkers moet bekend zijn wat de opvangprocedure inhoudt in hun instelling, waar ze naar toe kunnen voor een gesprek, wie eventueel vervangt als een opvang afwezig is en dergelijke.

Stap 4 Audits

De uitvoering van het Arbo-jaarplan, en dus ook de afgesproken maatregelen met betrekking tot de agressieproblematiek (veiligheid en opvang), dient regelmatig geëvalueerd te worden. In het kader van zo'n evaluatie (ook wel audit genoemd) moeten de volgende vragen aan de orde komen:

- Wat is er terecht gekomen van het gevoerde Arbo-beleid omtrent agressie? Worden de maatregelen in de praktijk wel uitgevoerd?
- Hoe vallen de getroffen maatregelen bij de werknemers? Zijn ze wel werkbaar en zijn er misschien nog andere maatregelen nodig?
- Zijn de doelstellingen gehaald en zo nee, waarom niet? En treden er wellicht ongewenste bij-effecten op?
- Wat zijn de consequenties hiervan voor het meerjarenplan?

Met behulp van zulke audits blijft het onderwerp onder de aandacht, kunnen knelpunten gesignaleerd worden en kunnen nieuwe verbeteringen doorgevoerd worden. Doel van zulke audits is dus niet alleen om het effect van de maatregelen te meten met behulp van de incidenten-registratie, maar met name om te zorgen dat agressie en geweld regelmatig onderwerp van gesprek is en blijft binnen de hele organisatie.

Bijlage 10

Aandachtspunten bij bouwkundige en elektronische beveiliging

10.1 Het selecteren van bouwkundige en elektronische maatregelen

10.1.1 Het programma van eisen

Door al in het ontwerp van een gebouw aandacht te besteden aan bouwkundige en elektronische beveiliging, kunnen criminaliteitsproblemen en later noodzakelijk blijken- de (dure) bouwkundige aanpassingen zoveel mogelijk voorkomen worden.

Het programma van eisen is in de ontwerpprocedure het meest geschikte moment om te zorgen dat er in het ontwerp aan preventie gedacht wordt: er kunnen concrete wensen en eisen in worden opgenomen. Ook het schetsplan en in mindere mate het definitieve plan lenen zich voor preventieve sturing.

Het is dus van belang dat de opdrachtgever of de voor de veiligheid en beveiliging verantwoordelijken zich al in een zo vroeg mogelijk stadium in het bouwteam uitspreken over hun wensen. Indien bij de opdrachtgever kennis en ervaring op beveiligingsgebied ontbreekt, zal op dat moment deskundigheid moeten worden ingehuurd.

In de reeks "Beveiliging van gebouwen" wordt uitgebreid ingegaan op de mogelijkheden van preventie in het ontwerpproces en op de bouwkundige en elektronische beveiliging van gebouwen. Met name deel 4 (bedrijfsgebouwen en terreinen) en deel 5 (kantoren) van deze reeks zijn voor zorginstellingen van belang. Deze publicaties worden uitgegeven door de Stichting Bouwresearch.

Inlichtingen over SBR-publicaties zijn in te winnen bij:

Stichting Bouwresearch

Postbus 1819

3000 BV ROTTERDAM

Telefoon: (010)4117276/4123528

Telefax: (010)4130175

10.1.2 Het Ruimte-risico-inschattingsmodel

Aangezien in zorginstellingen de risico's en dus de beveiliging per ruimte in het gebouw behoorlijk verschillen, zal men niet kunnen volstaan met het bepalen van de voor het gehele gebouw minimaal noodzakelijke maatregelen, maar zal men ook per ruimte/gebied zowel de risico's als beveiligingsmaatregelen moeten definiëren.

Met het Ruimte-risico-inschattingsmodel (Rrim) kunnen per ruimte van de zorginstelling de soorten risico's, de kans daarop en de ernst van de gevolgen worden ingeschat. Op grond hiervan kunnen prioriteiten worden bepaald en kan een beveiligingsbeleid worden uitgestippeld. Met behulp van het Rrim kunnen opdrachtgevers en ontwerper bij de (ver)bouw van een zorginstelling komen tot een rationeel beveiligingsplan dat in het verdere ontwerpproces meegenomen kan worden. Ook kan het Rrim worden gebruikt bij wijze van vooronderzoek, alvorens de kleurenmethode toe te passen. Het Rrim is in schema 1 weergegeven.

1 Gebouwonderdeel	2 Toegankelijk voor	3 Mogelijke risico's	4 Kans dat dit risico plaatsvindt (A=100% zeker)	5 Ernst van de gevolgen als dit risico (zie 3) plaatsvindt (1=rampzalig)	6 Prioriteit (=4+5)	7 Aanvullende preventieve maatregelen	8 Opmerkingen
Verpleegafdelingen							
Zusterposten							
Spogedeisende hulp (S.E.H.)							
Publieksruimten poli							
Operatie afdeling							
Technische ruimten							
Medicijnunits							
Magazijnen en archieven							
Postkamer en expeditie							
Computerruimten							
Bewakingsruimten							
Schoonmaak-ruimten							
Kantoorruimten							
Publieksruimten							
Balie							
Kantine en recreatieve ruimten							
Apotheek							
Behandeldkamers							
Röntgenafdeling							
Laboratoria							

10.1.3 De PIVA-ALRE-toets

Een hulpmiddel waarmee beoordeeld kan worden of een bepaalde combinatie van inbraakpreventieve maatregelen al dan niet zinvol is (zowel in de ontwerpfase als later), vormt de zogenaamde PIVA-ALRE-toets. Hierbij wordt het tijdsverloop van de vier fasen van inbraak, te weten Planning, de Inbraak zelf, de Verzameltijd voor de buit, en de Aftocht afgezet tegen het tijdsverloop van Alarmering en de Reactie van een hulpbiedende partij.

Deze toets maakt nog eens duidelijk dat het in bepaalde situaties volkomen zinloos is om elektronisch te alarmeren, omdat het bijvoorbeeld geruime tijd duurt voordat er eens iemand kan komen kijken en handelend op kan treden.

In praktische zin gebruikt men de toets om vooral met de bouwkundige maatregelen (de tijd verlengen voor Inbraak) en elektronische maatregelen (zo vroeg mogelijk, bij voorkeur nog vóór de Inbraak aanvangt) net zo lang te 'schuiven' tot een bevredigende verhouding in tijd is ontstaan tussen het moment van Inbraak en de Reactie. Bij een negatieve score van de toets blijken de fasen Planning en Aftocht het minste perspectief te bieden om de situatie te verbeteren. Daarentegen zijn het vooral de bouwkundige maatregelen (I) en een vroege alarmering (Al), alswel het verlengen van de Verzameltijd door organisatorische maatregelen, die tot een positieve bijdrage van het gewenste effect van beveiliging kunnen bijdragen.

10.2 Bouwkundige maatregelen

10.2.1 Algemene aandachtspunten

Het bouwkundig beveiligen van zorginstellingen komt in hoofdlijnen overeen met het bouwkundig beveiligen van andere soorten gebouwen. De volgende punten verdienen echter bij het ontwerpen en bouwkundig beveiligingen van een zorginstelling nadere aandacht:

Goede routing door het gebouw

De weg die de gebruikers moeten volgen, van buiten het gebouw naar de ruimte waar ze heen willen, maar ook van de ene naar de andere ruimte, moet duidelijk en overzichtelijk zijn. Dit om te voorkomen dat mensen te veel door het gebouw heen gaan zwerven. De routing kan ook gebruikt worden voor het sturen van de gebruikersgroepen bijvoorbeeld om bepaalde groepen gebruikers te weren van bepaalde lokaties en te voorkomen dat bezoekers op lokaties komen waar ze niet gewenst zijn.

Scheiding van functies

Als er in het gebouw functies zijn, die storend zijn voor andere functies of juist extra beschermd dienen te worden, moeten ze worden afgescheiden van die andere functies. Dat kan een kwestie zijn van geluidsisolatie, maar ook van strikte, ruimtelijke scheiding. Met een aparte ingang en misschien met eigen voorzieningen. Er moet gezorgd worden voor een goede onderlinge situering van de verschillende entrees. Zowel bij combinatie als bij scheiding van functies, moeten de interne routing en de al of niet nagestreefde scheiding naar buiten toe worden doorgezet. Buiten het gebouw moet dezelfde gedachtenlijn worden doorgezet naar voorzieningen buiten het gebouw. Ook functies in andere gebouwen kunnen van invloed zijn op het functioneren van de zorginstelling.

Flexibiliteit

Bij het ontwerpen van een gebouw op maat, wat door het specifieke gebruik van zorginstellingen noodzakelijk is, moet rekening gehouden worden met eventuele verande-

ringen in (deel)functies en omvang van het gebouw, die in de loop van de tijd kunnen optreden. Voor zover deze wijzigingen kunnen worden voorzien, kan daarop worden ingespeeld in het programma van eisen. Hierdoor zal een in de toekomst gewenste uitbreiding en ook verschuiving van functies eerder haalbaar worden.

Toch zullen vaak ook onvoorspelbare veranderingen optreden. Daarom moet het gebouw zodanig worden ontworpen en gebouwd, dat later wijzigingen met beperkte middelen kunnen worden ingevoerd, het liefst zonder ingrijpende verbouwingen. Als er toch verbouwd moet worden, moet dat budgettair geen onnodig negatieve consequenties hebben.

Uiterlijk

Bij het ontwerp voor het gebouw moet gestreefd worden naar een vriendelijk en prettig uiterlijk. Niet te open, maar zeker niet te gesloten. Er moeten degelijke materialen worden gebruikt, maar toch mag het gebouw niet op een bunker gaan lijken.

Enkele facetten van het uiterlijk die daarbij kunnen worden genoemd, zijn: de sfeer, de daglichttoetreding, de verlichtingssterkte, de entree, de logische opzet, de heldere routing, de keuzen van materialen en de zorgvuldige detaillering.

Sociale controle

Bij het plaatsen van een zorginstelling in een buurt of wijk moet worden gestreefd naar samenhang met andere functies, waardoor wederzijds een rol kan worden gespeeld bij preventie van schade. Woningen kunnen de sociale controle verzorgen voor voorzieningen als deze gesloten zijn. Om die reden zou kunnen worden overwogen een (beperkt) aantal woningen op het terrein van de zorginstelling te bouwen.

10.2.2 Belangrijke bouwkundige maatregel: Compartimentering

Een zorginstelling behoeft vrijwel nooit in z'n geheel zwaar te worden beveiligd. Men kan namelijk in het gebouw de risico-volle plekken isoleren van de rest en ze afzonderlijk een hogere graad van beveiliging meegeven. Deze benadering wordt aangeduid met de term 'compartimenteren'.

Compartimentering kan op verschillende schaalniveaus plaatsvinden. Zo kunnen binnen een zorginstelling hele functies (de apotheek, de opslag van patiëntengegevens) worden gecompartmenteerd. Met behulp van de kleurenmethode kan bekeken worden in hoeverre het beveiligingsniveau per ruimte of afdeling aansluit bij het risico-niveau (zie bijlage 1) en of het zinnig is bepaalde functies een hogere graad van beveiliging te geven.

Binnen deze (al dan niet gecompartmenteerde) functies kunnen weer bepaalde kleinere compartimenten worden gecreëerd: opbergruimten als de archiefkast, de medicijnkast etc. Op dit niveau kunnen de volgende typen compartimenten worden onderscheiden:

- 1 lockers en andere kasten voor het opbergen van persoonlijke eigendommen;
- 2 traditionele archiefruimten;
- 3 datakasten en datakluisen;
- 4 medicijnkasten;
- 5 kluisruimten en brand- en inbraakwerende kasten.

Teneinde te kunnen bepalen hoeveel opbergruimte van welk type er op welke plekken noodzakelijk is, dient de behoefte aan opbergmogelijkheden ingeschat te worden. Een hulpmiddel hierbij is om per type gebruiker te inventariseren wie wanneer wat waar wil opbergen¹¹. Schema 3 geeft een checklist die voor zorginstellingen van dienst kan zijn. De checklist is overigens slechts een eerste aanzet, die door de instelling zelf op maat moet worden gemaakt.

¹¹ Zie noten pagina 109

Checklist 'Wie bergt wanneer wat waarin op'

Wie?	Wat?	Waar?	Wanneer?
Personeel zorginstelling - verplegend personeel - artsen - SEH-personeel - baliepersoneel - administratie-personeel - kantine- en keukenpersoneel - etc.			
Diensten - technische dienst - schoonmakers - beveiligingsfunctionarissen - andere diensten			
Patiënten - poliklinische patiënten - SEH-patiënten - klinische patiënten			
Bezoekers - van polikliniek - van verpleegafdelingen - van de SEH - etc.			

De keuze voor een bepaald type compartiment hangt samen met de aard van het op te bergen goed en de mate van bescherming die het compartiment moet bieden. Om goed overleg te kunnen voeren met specialisten op dit gebied en een verantwoorde keuze te kunnen maken tussen de verschillende typen compartimenten die er in de aanbieding zijn, verdient het aanbeveling dat men zich enige basale (produkt)kennis eigen maakt. In het onderstaande zal deze basiskennis per type compartiment verschaft worden.

Traditionele archiefruimten

Het verdwijnen van gegevens op papier, microfilm of magnetische informatiedragers kan voor een zorginstelling rampzalig zijn. Het is dus duidelijk dat gegevens goed moeten worden beschermd. Bedacht moet echter worden dat goed ogende archief-ruimten vaak maar een zeer beperkte bescherming bieden, vooral wanneer de gegevens niet meer op papier staan.

Er dient daarom onderscheid gemaakt te worden in traditionele archiefruimten voor papieren zaken zoals boeken, rapporten, dossiers enz. en archief-ruimten die volledig zijn toegesneden op magnetische informatiedragers: de 'datakluizen'.

Deze laatste moeten we niet verwarren met de kluisruimten: dat zijn sterke inbraak- en brandwerende kluizen.

Traditionele archiefruimten moeten brand- en inbraakwerend worden uitgevoerd.

Hieronder volgen enkele tips voor adressen van instanties en naslagwerken op dit gebied waar men terecht kan voor nadere informatie en advies.

Adressen van relevante instanties:

- * Zeker bij zorginstellingen kan door opdrachtgevers of ontwerpers advies worden ingewonnen bij de Provinciale Archiefinspecteur, gevestigd in het Provinciehuis van de betreffende provincie.
- * Voorts is er nog een Landelijk Overleg Provinciale Archiefruimten (Postbus 122, 9400 AC Assen) waar nadere informatie kan worden ingewonnen.

Relevante naslagwerken:

- * Een goede referentie voor de uitvoering van traditionele archiefruimten 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 de ligging van het gebouw, bouwkundige voorzieningen, brandbeveiligingen klimaatbeheersing. Het voorschrift behandelt niet de inbraakwerendheid.
- * Een bruikbare referentie voor ontwerpers van archiefruimten is voorts hoofdstuk 5000 'Archiefbeheer/bouwzaken' uit het 'Handboek archiefbeheer in de praktijk' (Samson).
- * Duitsland kent een norm voor de bouw van archiefruimten, de DIN 4102. 'Empfehlungen für den Bau von Archivräumen' kan gratis worden aangevraagd bij het Forschungs- und Prüfungsgemeinschaft Geldschränke und Tresoranlagen e.V., Postfach 710864, D- 6000 Frankfurt 71.

105

Data-kasten en datakluisen

Papier kan in een data-kast de gevolgen van een brand relatief goed doorstaan. Magnetische informatiedragers zijn echter erg gevoelig voor temperatuurstijgingen en verhogingen van de relatieve vochtigheidsgraad. Zo dient men magnetische informatiedragers bijvoorbeeld niet te beschermen in kluisen met dikke betonnen wanden. Vocht uit het beton zal bij brand namelijk als waterdamp in de kluis terechtkomen. De relatieve vochtigheid loopt daardoor op tot boven de 85%, de fatale grenswaarde voor magnetische informatiedragers.

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 Duitse VDMA-normen o.g.¹².

Grotere concentraties databestanden dienen te worden opgeborgen in daarvoor bestemde datakluisen. Datakluisen beschermen de inhoud tegen brand, rook, water(damp), in- en uitstraling van hoogfrequent-signalen, magnetische stralen en zijn verder explosie- en inbraakwerend.

De Duitsers hebben met de VDMA-normen en bijbehorende klasseringen de datakasten en kluisen 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.

¹² Zie noten pagina 109

Medicijnkasten

Aan het opbergen van geneesmiddelen worden extra wettelijke eisen gesteld, waar zorginstellingen zich aan dienen te houden. Zo is het wettelijk verplicht om opiaten op te bergen in aparte afsluitbare ruimten (medicijnkasten bijvoorbeeld).

De regelgeving omtrent de opslag van opiaten wordt nader behandeld in de volgende publikatie:

Geestverruiming opgeborgen

Caro Vermeulen

Van Dijk, Van Soomer en Partners

in opdracht van het Landelijk Bureau Voorkoming Misdrijven

106

Kluisruimten en brand- en inbraakwerende kasten

Voor het opbergen van zeer waardevolle goederen zijn verschillende kluisen op de markt. Het beoordelen van de kwaliteit van kluisen en brandkasten is een specialistische zaak.

De Stichting Kwaliteitsbeoordeling Brandkasten (SKB) geeft een lijst uit met alle brandkasten en kluisen die op de markt zijn, aangevuld met aanbevelingen omtrent de maximale waarde die in de verschillende typen brandkasten opgeborgen mag worden.

Deze lijst is op te vragen bij:

Stichting Kwaliteitsbeoordeling Brandkasten

Postbus 85674

2508 CL 's-Gravenhage

Tel: (070)3738225/3943152

10.3 Elektronische maatregelen

Elektronische maatregelen dienen zeer nauw afgestemd te worden op organisatorische maatregelen en procedures. Ook dienen de elektronische en bouwkundige maatregelen goed op elkaar afgestemd te worden. Gebruikersvriendelijkheid dient voorop te staan, aangezien dit de effectiviteit van de maatregelen vergroot.

Al met al betekent dit dat ontwerpers met de volgende aspecten rekening moeten houden:

*Ergonomische aspecten*¹³

Dit speelt met name bij de camera-bewaking. De manier waarop de monitors staan opgesteld blijkt namelijk van invloed te zijn op de kwaliteit van de waarneming en dus op de effectiviteit van het systeem. In dit verband zijn de volgende tips te geven over de opstelling van de monitors in de beveiligingsruimte.

- * Monitoren zijn beschikbaar in diverse beeldformaten. Voor het juiste formaat is de kijkafstand bepalend. Gerekend moet worden op een kijkafstand van ongeveer vijf à zes keer het beeldschermformaat.
- * Bij de opstelling van een monitor moet erop worden gelet dat invallend licht geen spiegelingen op het beeldscherm veroorzaakt.
- * Wanneer meerdere monitoren op één rij worden geplaatst is het aan te bevelen de kijkhoek niet groter te maken dan 45 graden. Als slechts één persoon hoeft waar te nemen kan het voordelen bieden de monitoren in paraboolvorm op te stellen.

¹³ Zie noten pagina 109

Wanneer monitoren boven elkaar worden geplaatst is het aan te bevelen de kijk hoek niet groter dan 30 graden te maken. Dezelfde regels dienen te worden gehanteerd wanneer meerdere personen moeten waarnemen.

Organisatorische aspecten

Bij alle elektronische beveiligingssystemen, of het nu een CCTV-systeem is of een inbraakdetectiesysteem, moeten niet alleen het ontwerp, de componenten en de installatie van het systeem zonder meer uitstekend zijn, maar zeer beslist ook de organisatie en procedures daaromheen. Aan dit laatste ontbreekt het helaas nogal eens. Procedures zijn essentieel om te waarborgen dat het systeem onder alle omstandigheden goed functioneert en dat er snel en adequaat gereageerd wordt op een alarmering. In dit verband dient het laatste deel van de PIVA-ALRE-toets in gedachte te worden gehouden: een snelle alarmering heeft alleen nut als die ook opgevolgd wordt door een snelle reactie.

De aanschaf van een alarmsysteem dient daarom gepaard te gaan met een goede instructie en motivatie van het personeel omtrent aspecten als het inschakelen van het systeem en het reageren op alarmeringen. Ook het maken van goede afspraken met externe instanties als politie en brandweer is hier essentieel.

Verder dient er gezorgd te worden voor noodvoorzieningen voor het geval er stroomstoringen optreden.

Bouwkundige ontwerp-technische aspecten

Voor de bouwkundig ontwerper is van belang dat in een zo vroeg mogelijk stadium alle bouwkundige details voor bijvoorbeeld het CCTV-systeem worden vastgelegd zoals sparingen, kabeldoorvoeren, bevestigingspunten voor camera's, voldoende (loze) leidingen, een voldoende grote ruimte voor de opstelling van monitoren en eventueel andere beveiligingsapparatuur.

In het algemeen kan gesteld worden dat het op juiste wijze selecteren en installeren van elektronische beveiligingsmiddelen zeer specialistisch werk is.

Nadat door de bouwkundig ontwerper en zijn opdrachtgever een ruwe schets is gemaakt van de gewenste beveiliging, is het daarom zaak om in een zo vroeg mogelijk stadium van nieuwbouw of verbouw een deskundige te raadplegen. Dat kan via de 'eigen' E-installateur en/of een erkend beveiligingsbedrijf. Daarbij is het van belang dat wordt bedongen dat de produkten uiteraard kwalitatief uitstekend en bij voorkeur van één merk moeten zijn, maar vooral moeten worden betrokken via een fabrikant of importeur met eigen technische adviseurs op dit vakgebied. Eventueel kan de installateur in samenwerking met de fabrikant of de importeur het systeem opleveren en garanderen.

NOTEN

- 1 Zie de rapportage Beveiliging Ziekenhuizen Regio Twente, DamhuisElshoutVerschure, Den Bosch, 1995.
- 2 Wat ziekenhuizen betreft blijkt dit uit de uitkomsten van het onderzoek Criminaliteit in en rond ziekenhuizen; een landelijk onderzoek naar criminaliteit, beveiliging en onveiligheidsgevoelens. H. Oosten, Schalke & Partners in opdracht van de Directie Criminaliteitspreventie van het Ministerie van Justitie, februari 1993.
- 3 Criminaliteit in en rond ziekenhuizen; een landelijk onderzoek naar criminaliteit, beveiliging en onveiligheidsgevoelens. H. Oosten, Schalke & Partners in opdracht van de Directie Criminaliteitspreventie van het Ministerie van Justitie, februari 1993.
- 4 Uit het DCP-onderzoek Criminaliteit in en rond ziekenhuizen blijkt dat circa 90% van de onderzochte instellingen geen formele opvangprocedure kennen voor personeel, patiënten en bezoekers die slachtoffer waren geworden van criminaliteit in het ziekenhuis of tijdens het verrichten van werkzaamheden voor het ziekenhuis.
- 5 DCP, 1993.
- 6 Schatting van de VBN in het tijdschrift Werk in bewaking, maart 1995, blz. 8.
- 7 DSP, 1993
- 8 Zie ook bijlage 9.
- 9 Er lijken minder raakvlakken te bestaan tussen milieuzorg en beveiliging, zodat de milieuzorg hier verder buiten beschouwing wordt gelaten.
- 10 Zie ook hoofdstuk 2.
- 11 Bedacht moet worden dat er ook wettelijke verplichtingen op dit gebied bestaan (zie onder meer de Wet op de persoonsregistratie).
- 12 De VDMA-norm 24991, deel 2, heeft betrekking op de Databescherming tegen brand, en de VDMA 24992 op inbraak. Aan het label van de VDMA-norm valt af te lezen voor welk type goederen het geschikt is. VDMA label P is voor papier, label D is voor tapes en schijven, label DIS voor diskette. Wanneer een produkt 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 op het merkplaatje van een produkt staan. Overigens zullen brandkasten, datakluisen e.d. te zijner tijd onder de Europese regelgeving komen te vallen. Op dit moment zijn de activiteiten op het gebied van Europese normering (harmonisatie) nog volop in beweging. Vooralsnog kan echter de VDMA-klassering als goede referentie worden gehandhaafd.
- 13 Overigens zijn er nog andere redenen om aan dit aspect aandacht te besteden dan vanuit beveiligingsoogpunt. De Arbo-wet stelt namelijk ook de nodige ergonomische eisen aan de werkomgeving van werknemers.

Bijlage 11

Samenvatting brandbeveiligingsconcept gezondheidszorggebouwen

Brandbeveiligingsconcept

gezondheidszorggebouwen

Alleen hoofdstuk 4 en 5

Ministerie van Binnenlandse Zaken

Directie Brandweer en Rampenbestrijding

Afdeling Preventiebeleid

Den Haag, (herdruk) augustus 1995

Doelstellingen van de brandbeveiliging

van gezondheidszorggebouwen

4

H o o f d s t u k

4.1 Doelstellingen

Het resultaat van de analyse, uitgevoerd in hoofdstuk 3, vormt de basis voor de

legitimering van de doelstellingen, die voor de verdere ontwikkeling van dit

brandbeveiligingsconcept noodzakelijk zijn. Deze doelstellingen zijn:

- 1 Het zoveel mogelijk voorkomen van doden en/of gewonden met blijvend letsel en het zoveel mogelijk beperken van het aantal gewonden zonder blijvend letsel bij brand.
- 2 Een brand in een gezondheidszorggebouw moet zodanig beheersbaar zijn, dat – zowel direct als indirect – zo min mogelijk nadelig effect, buiten een vooraf bepaald gebied ontstaat.

4

De doelstellingen worden hierna nader beschouwd met als uiteindelijk doel in hoofdstuk 5 de brandbeveiligingsmaatregelen en -voorzieningen te kunnen formuleren.

Om dat te kunnen doen wordt gebruik gemaakt van het normatief brandverloop in een gezondheidszorggebouw, dat als referentiemodel kan worden toegepast.

4.2 Normatief brandverloop in een gezondheidszorggebouw

Het normatief brandverloop is afhankelijk van het type gezondheidszorggebouw. Onderscheiden worden gebouwen waarin zelfredzame patiënten verblijven (in principe alleen overdag in gebruik) en gebouwen waarin een groot deel van de patiënten tot zelfs alle patiënten niet-zelfredzaam zijn (ook 's nachts in gebruik).

Bij een brand speelt het element tijd een belangrijke rol. Er is sprake van een tijdtrace tussen enerzijds branduitbreiding plus rookverspreiding en anderzijds ontdekking, redding, ontruiming en blussing. De temperatuursontwikkeling van een brand, die in de figuren 4.2 en 4.4 is weergegeven, is niet evenredig met het tijdsverloop.

Na een trage ontwikkeling in het begin, waarbij de temperatuur in de ruimte langzaam oploopt, ontwikkelt de brand zich opeens zeer snel, waarbij de temperatuur in de ruimte eveneens snel oploopt (punt van vlamoverslag). Het temperatuur-tijdsverloop van een brand is gemodelleerd weergegeven. Deze modellering komt, met uitzondering van de eerste ontwikkelingsfase van een brand, overeen met de standaardbrandkromme (zie figuur 4.1).

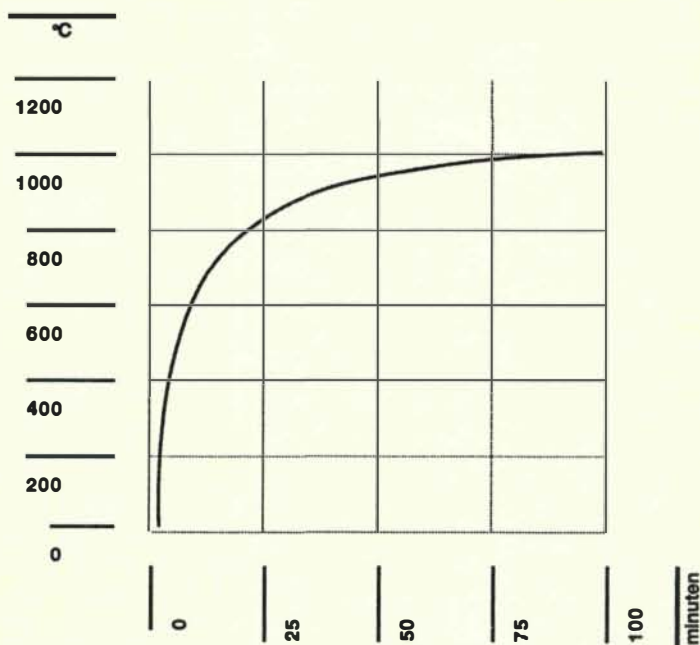
Zo'n brand zal zich kunnen voordoen in een onbemande ruimte, of in een ruimte waar iemand aanwezig is die de brand niet wil of kan melden.

De toepassing van een temperatuur-tijdsverloop voor het normatief brandverloop dat grote overeenkomsten vertoont met de standaardbrandkromme is gerechtvaardigd.

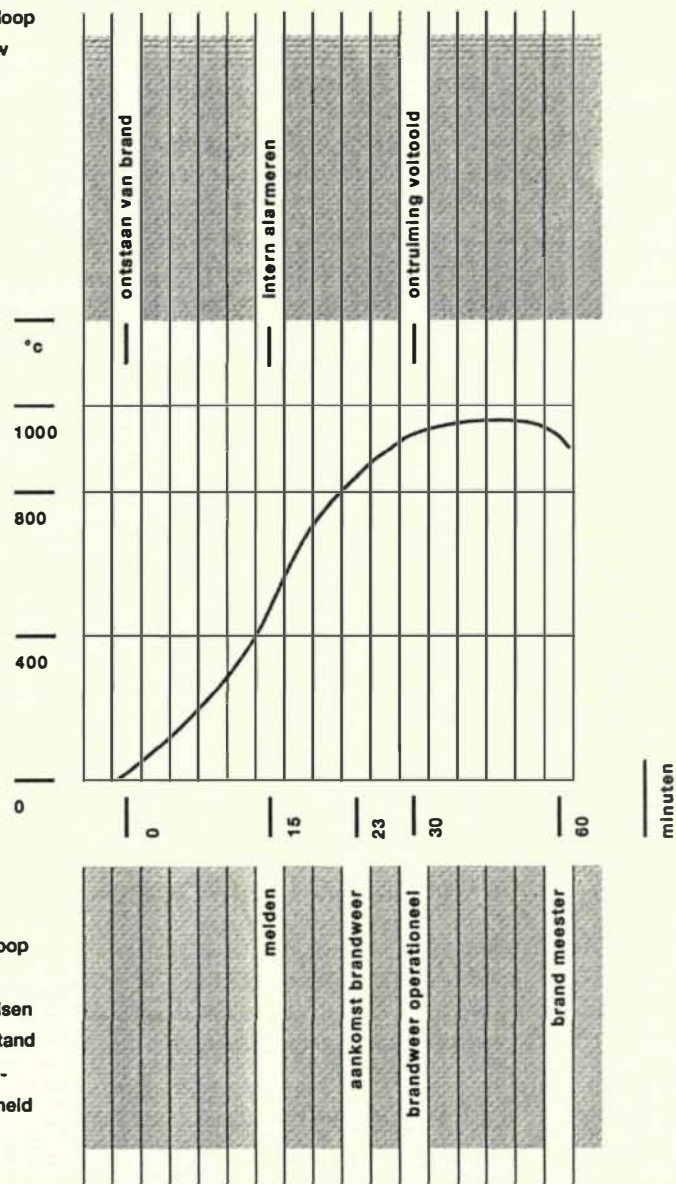
De reden hiervan is dat de indeling van een gezondheidszorggebouw en de hierin te verwachten variabele en permanente vuurbelasting in geval van brand over het algemeen zal leiden tot een brandverloop, dat grote overeenkomsten vertoont met de standaardbrandkromme.

5

Figuur 4.1 De standaard brandkromme



**Figuur 4.2 Normatief brandverloop
in een gezondheidszorggebouw
met zelfredzame patiënten**



De bij het normatief brandverloop genoemde tijden zijn geen grenswaarden van prestatie-eisen en geven dan ook geen weerstand tegen branddoorslag en brandoverslag, of een brandwerendheid tot bezwijken weer.

Uitgangspunten van het normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten

Hierbij is ervan uitgegaan, dat in dat deel van het gezondheidszorggebouw geen personen aanwezig zijn en de brand wordt ontdekt door personen in andere delen van het gebouw of in de omgeving van het gebouw op het moment van vlamoverslag in de brandruimte, wanneer daarbij (onder veel lawaai) de ruiten breken en de vlammen naar buiten slaan. Zijn er wel personen in het betreffende deel van het gezondheidszorggebouw aanwezig, dan kan de ontdekkings tijd korter zijn.

Bij het normatief brandverloop in een gezondheidszorggebouw wordt ervan uitgegaan dat:

- binnen 15 minuten na het ontstaan van een brand, de brand is ontdekt en gemeld aan de bedrijfshulpverleners en alarmering van de in het gebouw aanwezige personen en melding aan de brandweer heeft plaatsgevonden;

Doordat tijdens het vluchten de trappehulsdeuren – voor het onmiddellijk passeren (vluchten) van personen – één of meerdere malen worden geopend, zal de rook vanaf de verdieping van de brand in het trappenhuis doordringen en wel op een zodanige wijze dat gedurende ten minste 30 minuten na het ontstaan van brand het trappenhuis is gevrijwaard van grote hoeveelheden rook.

Uitgaande van een opkomsttijd voor dit type gezondheidszorggebouwen van 8 minuten, resteert een inzettijd van maximaal 7 minuten.

Daar in de 'handleiding Brandweezorg' gezondheidszorggebouwen met zelfredzame patiënten niet worden vermeld, is aansluiting gezocht bij gebouwsoorten met een gelijksoortige populatie (scholen, winkels). De daarbij genoemde waarde is overgenomen.

- binnen 15 minuten na alarmering moeten de door de brand bedreigde personen al dan niet met hulp van de bedrijfshulpverleners doch zonder hulp van de brandweer kunnen vluchten naar een veilige plaats buiten het gezondheidszorggebouw. Met andere woorden: door brand bedreigde personen moeten binnen 30 minuten na het ontstaan van de brand zonder hulp van de brandweer het gebouw hebben kunnen verlaten.
- binnen 15 minuten na het melden van de brand aan de brandweer alarmcentrale de brandweer aanwezig en operationeel is (water op het vuur).

7

Academisch Ziekenhuis Lelden (5-4-'94)



Om de brand beheersbaar te houden, mag de brand niet buiten een vooraf bepaald gebied van een gezondheidszorggebouw treden. Uitgaande van het normatief brandverloop in dit type gezondheidszorggebouwen betekent dit, dat doorgaans tussen dit gebied en naast-, boven- en onderliggende gebieden een constructie aanwezig is, waardoor gedurende 60 minuten een in dat gebied begonnen brand niet naar het andere gebied overslaat. In de praktijk blijkt 60 minuten een redelijk haalbare tijd.

- de brandweer de brand binnen 60 minuten na het ontstaan onder controle moet hebben (anders gezegd: de brand meester zijn). Op dat moment behoren alle door de brand bedreigde personen te zijn gered. Met andere woorden, er wordt van uitgegaan, dat de brandweer binnen 30 minuten na het operationeel zijn, de zich nog in het bedreigde gebied bevindende personen heeft gered en verdere uitbreiding van de brand in beginsel heeft voorkomen.

Bij het normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten kunnen de volgende fasen worden onderscheiden:

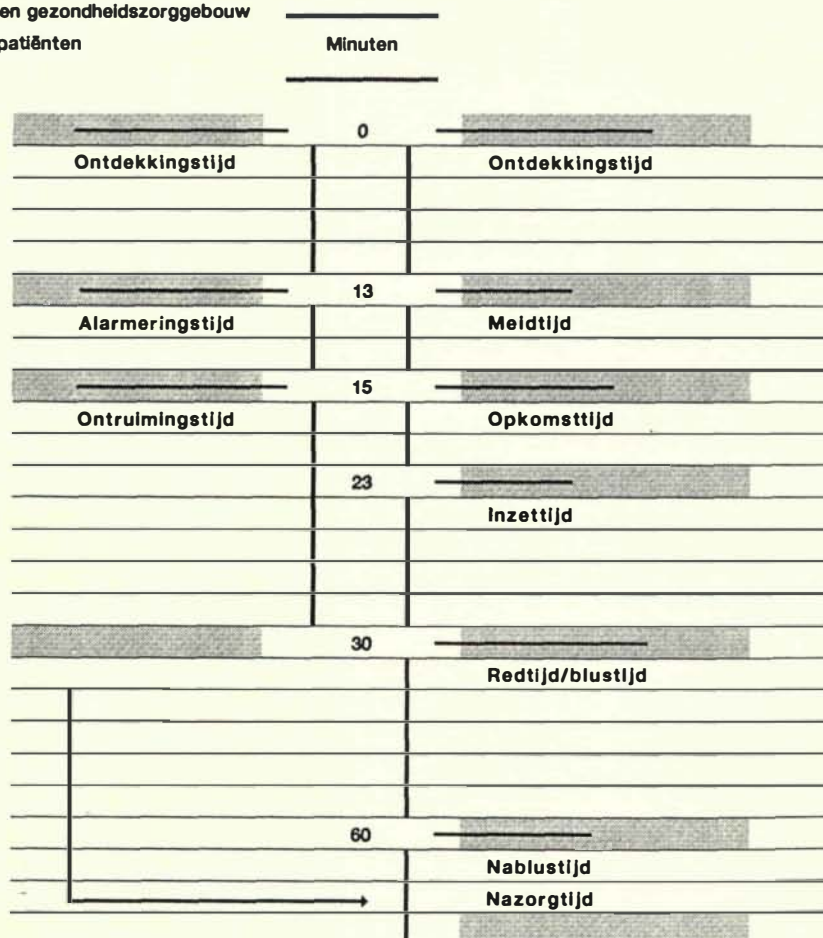
- 1 De ontdekkingstijd.
- 2 De alarmeringstijd (waarschuwen bedrijfshulpverleners en overige in het gebouw aanwezige personen).
- 3 De ontruimingstijd.
- 4 De meldtijd (aan de alarmcentrale van de brandweer).
- 5 De opkomsttijd van de brandweer:
 - a de verwerkingstijd van de brandmelding op de brandweeralarmcentrale
 - b de uitruktijd, de tijd die het personeel van de brandweer nodig heeft om het brandweervoertuig te bezetten;
 - c de rijtijd.
- 6 De inzettijd van de brandweer.
- 7 De red- en blustijd van de brandweer.
- 8 De nablustijd.
- 9 De nazorgtijd.

8

Deze fasen worden schematisch weergegeven in figuur 4.3.

Voor wat betreft de definiëring van de genoemde tijden is zoveel mogelijk aansluiting gezocht bij reeds bestaande definities. Echter ten aanzien van 4 'de meldtijd' wordt opgemerkt dat de handleiding Brandweezorg dit begrip hanteert voor 5a 'de verwerkingstijd'. Er zal naar worden gestreefd de handleiding in overeenstemming te krijgen met de definities van het brandbeveiligingsconcept.

Figuur 4.3 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten



Uitgangspunten van het normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten

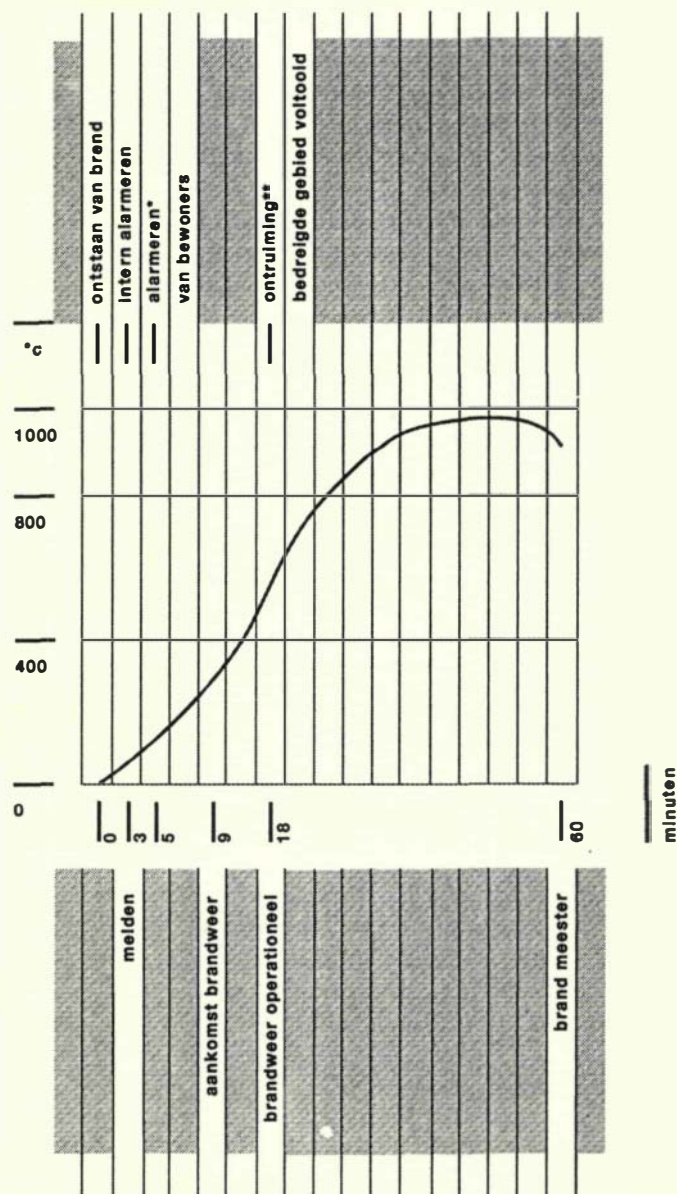
Hierbij is ervan uitgegaan, dat in het gezondheidszorggebouw een brandmeldinstallatie met volledige bewaking en directe doormelding naar de brandweeralarmcentrale aanwezig is en dat alarmering van de bedrijfshulpverleners automatisch, zonder tussenkomst van derden, gebeurt.

Hierbij is ervan uitgegaan, dat de bedrijfshulpverleners binnen 2 minuten met minimaal 2 personen bij de brandende ruimte zijn aangekomen en dat de patiënt(en) daarna binnen 2 minuten naar een veilige plaats is/zijn gebracht en de deur van de brandende ruimte wordt gesloten.

Bij het normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten wordt ervan uitgegaan dat:

- binnen 1 minuut na het ontstaan van een brand, de brand is ontdekt en alarmering van de bedrijfshulpverleners en melding aan de brandweer heeft plaatsgevonden;
- binnen 4 minuten na het melden van de brand de patiënt(en) vanuit de brandende kamer naar een veilige plaats is/zijn gebracht.

Figuur 4.4 Normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten



Het gebied moet in principe zijn ontruimd, voordat met de brandbestrijding wordt begonnen. Op dat moment gaat namelijk de deur van de brandruimte weer open en komen grote hoeveelheden rook de gang op.

Uitgaande van een opkomsttijd voor gezondheidszorggebouwen voorzien van een brandmeldinstallatie met volledige bewaking overeenkomstig de 'handleiding Brandweezorg' van 8 minuten, resteert een inzetijd van maximaal 7 minuten.

In afwijking van het gestelde in de 'handleiding Brandweezorg' is voor alle gezondheidszorggebouwen met niet-zelfredzame patiënten de waarde voor nieuwe ziekenhuizen met een brandmeldinstallatie met volledige bewaking aangehouden.

Daar de kans dat in dit type gebouwen reddend moet worden opgetreden door de brandweer groter is dan in andere type gebouwen en er in dat geval dus minder tijd over is om daadwerkelijk te blussen, is er van uitgegaan dat er meer tijd nodig is om de brand onder controle te krijgen.

Om de brand beheersbaar te houden, mag de brand niet buiten een vooraf bepaald gebied van een gezondheidszorggebouw treden.

Uitgaande van het normatief brandverloop in gezondheidszorggebouwen betekent dit, dat doorgaans tussen dit gebied en naast-, boven- en onderliggende gebieden een constructie aanwezig is, waardoor gedurende 60 minuten een in dat gebied begonnen brand niet naar het andere gebied overslaat. In de praktijk blijkt 60 minuten een haalbare tijd.

Proefneming ziekenhuis, Rotterdam

■ binnen 15 minuten na alarmering van de bedrijfs-hulpverleners de patiënten uit het bedreigde gedeelte van het gezondheidszorggebouw moeten zijn gehaald, waarna deze patiënten worden overgebracht naar een veilige plaats.

■ binnen 15 minuten na het melden van de brand aan de brandweeralarmcentrale de brandweer aanwezig en operationeel is (water op het vuur).

■ de brandweer de brand binnen 60 minuten na het ontstaan onder controle moet hebben (anders gezegd: de brand meester zijn). Op dat moment moeten alle door de brand bedreigde personen zijn gered. Met andere woorden, de brandweer moet binnen 44 minuten na het operationeel zijn, de door bijzondere omstandigheden zich nog in het bedreigde gebied bevindende personen hebben gered en verdere uitbreiding van de brand in beginsel kunnen voorkomen.

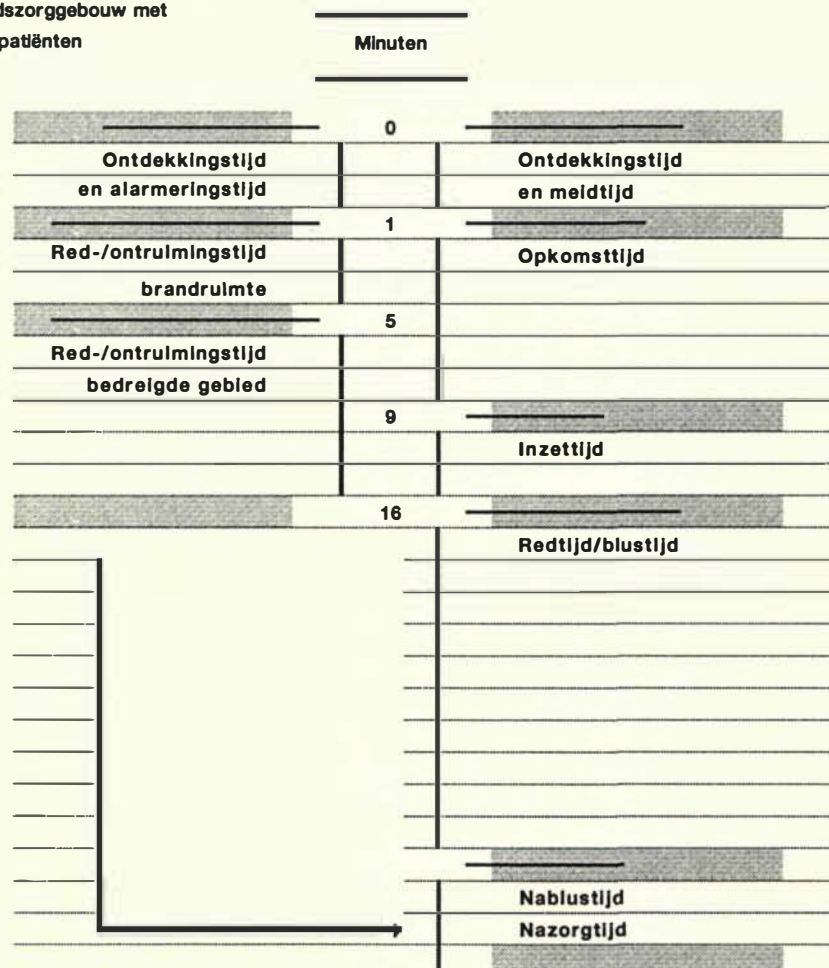
Bij het normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten kunnen de volgende fasen worden onderscheiden:

- 1 De ontdekkingstijd.
- 2 De alarmeringstijd (waarschuwen bedrijfshulpverleners in een gezondheidszorggebouw).
- 3 De red-/ontruimingstijd van de brandruimte.
- 4 De red-/ontruimingstijd van het bedreigde gebied.
- 5 De meldtijd (aan de alarmcentrale van de brandweer).
- 6 De opkomsttijd van de brandweer:
 - a de verwerkingstijd van de brandmelding op de brandweeralarmcentrale
 - b de uitruktijd, de tijd die het personeel van de brandweer nodig heeft om het brandweervoertuig te bezetten;
 - c de rijtijd.
- 7 De inzettijd van de brandweer.
- 8 De red- en blustijd van de brandweer.
- 9 De nablustijd.
- 10 De nazorgtijd.

11

Deze fasen worden schematisch weergegeven in figuur 4.5.

**Figuur 4.5 Fasen in een normatief brandverloop
In een gezondheidszorggebouw met
niet-zelfredzame patiënten**



4.3 Gebeurtenissenboom van een brand

Het verloop van brand in een gezondheidszorggebouw kan schematisch in de vorm

van een gebeurtenissenboom worden weergegeven (zie figuur 4.6).

In deze figuur worden in de meest logische volgorde de diverse stadia van een

brand met de daarbij behorende acties aangegeven vanaf het ontstaan van de

brand tot het moment dat de brand onder controle is (brand meester)

12

en de nazorg.

Dit zijn de

gebeurtenissen.

Nablussen als zodanig wordt niet nader als gebeurtenis opgenomen.

Ten aanzien van de daadwerkelijke nazorg kan worden opgemerkt, dat deze over het algemeen aanvangt na het moment, dat de brand onder controle is.

Echter specifieke acties, gericht op de voorbereiding van nazorg, kunnen in diverse fasen van het nonmatief brandverloop aanvangen.

In de gebeurtenissenboom is een driedeling aangebracht, waarbij zoveel mogelijk is getracht de gebeurtenissen naar discipline te groeperen, te weten:

gebeurtenissen (acties) gericht op de gebruikers van het gebouw, de eventueel aanwezige automatische blusinstallatie(s) en de brandweer.

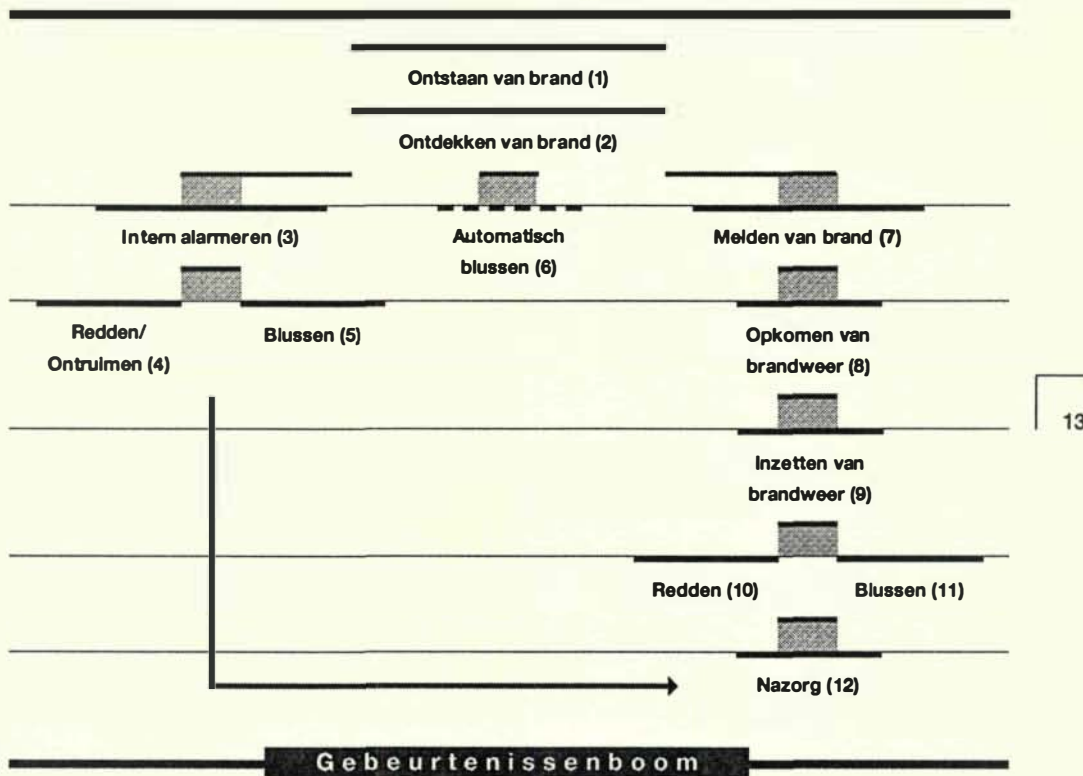
Sommige van deze acties beperken zich niet strikt tot een bepaalde discipline, zoals het melden van brand en de nazorg.

Van elke gebeurtenis in deze boom is in principe een specifieke doelstelling af te leiden. Deze specifieke doelstellingen kunnen worden bestudeerd en gerubriceerd, met als doel maatregelen en voorzieningen op hoofdlijnen te kunnen formuleren (zie hoofdstuk 5).

Het spontaan doven van een brand is als gebeurtenis niet opgenomen in de gebeurtenissenboom. Het weglaten hiervan is verantwoord, daar het geen invloed heeft op de maatregelen en voorzieningen op hoofdlijnen. Hoe eerder wordt ingegrepen in het verloop van de gebeurtenissen die bij een brand een rol spelen, des te geringer zijn de gevolgen. Met andere woorden: indien de eerste gebeurtenis – het ontstaan van brand – kan worden voorkomen, zullen ter realisatie van de doelstellingen op een lager niveau geen maatregelen meer behoeven te worden genomen. Immers het ontstaan van brand voorkomen, is de meest effectieve maatregel. Indien men uitsluitend onbrandbare materialen gebruikt kan er ook geen brand ontstaan.

Voor het geval dat men maatregelen treft, die van invloed zijn op een latere gebeurtenis (er is dan brand), bestaat de kans dat de doelstellingen niet worden gerealiseerd. Om dit toch te bereiken zullen gelijktijdig maatregelen moeten worden getroffen, die andere (latere) gebeurtenissen in positieve zin beïnvloeden. In de gebeurtenissenboom van een brand treedt een aantal gebeurtenissen, die in aard overeenstemmen, naast elkaar op. Nadat een brand is ontdekt, worden er zowel door de interne organisatie in een gezondheidszorggebouw als door de (gemeentelijke) brandweer (gelijktijdig) acties ondernomen. De wijze waarop de interne organisatie optreedt bij brand is van directe invloed op de actie die de brandweer zal moeten nemen. Als bijvoorbeeld de bedrijfshulpverleners van het gezondheidszorggebouw er in slagen het bedreigde gebied te ontruimen en de brand te blussen, zal de taak van de brandweer zich beperken tot een nacontrole. Als de interne organisatie hierin niet slaagt, is de inzet van de brandweer heel belangrijk.

Figuur 4.6 Gebeurtenissenboom van een brand



4.4 Vaststellen van specifieke doelstellingen

De volgende specifieke doelstellingen kunnen uit de gebeurtenissenboom worden afgeleid. De getallen verwijzen naar de getallen in de gebeurtenissenboom.

- 1 Het voorkomen van brand.
- 2 Het zo snel mogelijk ontdekken van brand.
- 3 Het zo snel en adequaat mogelijk alarmeren van
 - a bedrijfshulpverleners en overige personen in een gezondheidszorggebouw met zelfredzame patiënten;
 - b bedrijfshulpverleners in een gezondheidszorggebouw met niet-zelfredzame patiënten.
- 4 Het tijdig
 - a ontruimen van een gezondheidszorggebouw met zelfredzame patiënten;
 - b redden/ontruimen van personen door bedrijfshulpverleners van een gezondheidszorggebouw met niet-zelfredzame patiënten.
- 5 Het blussen van een beginnende brand door bedrijfshulpverleners/personeel van een gezondheidszorggebouw.
- 6 Het zo snel mogelijk automatisch blussen van brand.
- 7 Het zo snel mogelijk melden van brand aan de alarmcentrale van de brandweer.
- 8 Het zo snel mogelijk opkomen van de brandweer.
- 9 Het zo snel en adequaat mogelijk inzetten van de brandweer.
- 10 Het zo snel mogelijk in veiligheid brengen van personen, die zich nog in het bedreigde gebied bevinden.
- 11 Het zo snel en adequaat mogelijk blussen van de brand.
- 12 Het zo snel en adequaat mogelijk voorzien in nazorg.

Hierna worden de specifieke doelstellingen verder uitgewerkt met het oog op het vaststellen van de brandbeveiligingsmaatregelen en -voorzieningen op hoofdlijnen in hoofdstuk 5. Per specifieke doelstelling wordt aangegeven met welke aspecten rekening dient te worden gehouden bij het vaststellen van de brandbeveiligingsmaatregelen en -voorzieningen op hoofdlijnen.

De hierbij per aspect genoemde lijst omstandigheden/mogelijkheden is niet limitatief, doch geeft een indruk.

4.4.1 Het voorkomen van brand

Teneinde te weten te komen hoe een brand kan worden voorkomen, moet worden nagegaan hoe brand kan ontstaan. Er van uitgaande dat in een gezondheidszorggebouw brandbaar materiaal aanwezig is, kan brand ontstaan door:

1 Het gebruiken van open vuur

Het onder normale omstandigheden gebruiken van open vuur kan in gezondheidszorggebouwen voorkomen in de volgende situaties:

- voor verwarmingsdoeleinden (kachels, CV-ketels en dergelijke)
- voor kookdoeleinden (fornuis, gasstel en dergelijke)
- voor sfeerverlichting (kaarsen, lampions en dergelijke)
- roken
- bij werkzaamheden (lassen, verf afbranden, dakdekken en dergelijke)
- laboratoriumproeven (bunsenbrander en dergelijke).

2 Het misbruiken van open vuur

Het misbruiken van open vuur kan in gezondheidszorggebouwen in de volgende situaties voorkomen:

- opzettelijke brandstichting
- niet opzettelijke brandstichting, bijvoorbeeld spelen met vuur of baldadigheid.

3 Het blootstaan aan vlieg vuur en/of straling

Een gezondheidszorggebouw kan worden blootgesteld aan vlieg vuur en/of straling als een ander bouwwerk of materiaal in de naaste omgeving van het gezondheidszorggebouw in brand staat.

4 Door verhitting, zonder dat er sprake is van open vuur

Verhitting van materialen, constructieonderdelen en dergelijke, kan in gezondheidszorggebouwen onder de volgende omstandigheden voorkomen:

- bij de afvoer van hete rookgassen van kachels, CV-ketels en dergelijke
- bij elektrische installaties, die veel warmte ontwikkelen (verlichtingsspots nabij gordijnen en/of versiering en dergelijke)
- door chemische reacties (laboratoriumproeven en dergelijke).

5 Storing in, danwel defecten aan technische installaties en apparatuur

Storing in, danwel defecten aan technische installaties en apparatuur kunnen ontstaan door:

- het uitvallen van (thermische) beveiligingen
- het optreden van elektrische sluitingen
- het ondeskundig aanleggen of installeren
- geen of slecht onderhoud.

6 Blikseminslag

Met name hoge of afgelegen gezondheidszorggebouwen hebben een verhoogde kans op blikseminslag.

Een brand wordt pas als ontdekt beschouwd, wanneer degene die de brand opmerkt een daadwerkelijke actie pleegt, waardoor er vervolgacties plaatsvinden. Met andere woorden, wanneer iemand brand sticht en vervolgens niets doet, wordt de brand nog niet als ontdekt beschouwd.

4.4.2 Het zo snel mogelijk ontdekken van brand

Het ontdekken van brand kan op de volgende manieren plaats vinden:

1 Zonder technische hulpmiddelen

De mens kan brand ontdekken door zintuiglijke waarneming:

- het zien van rook en/of vuur
- het ruiken van een brandlucht
- het proeven van een rooksmaak
- het voelen van een snelle ongewone toename van temperatuur
- het horen van brand (knetteren van hout, de explosie ten gevolge van de vlamoverslag en dergelijke).

2 Met technische hulpmiddelen

Door het gebruik van technische hulpmiddelen, die één of meerdere van de volgende brandverschijnselen signaleren:

- rook (beperking zicht, samenstelling van de rook en dergelijke)
- temperatuur(sverhoging)
- vlammen
- geluid.

15

4.4.3 Het zo snel en adequaat mogelijk alarmeren van

- a bedrijfshulpverleners en overige personen in een gezondheidszorggebouw met zelfredzame patiënten
- b bedrijfshulpverleners in een gezondheidszorggebouw met niet-zelfredzame patiënten

Het alarmeren van bedrijfshulpverleners en overige personen in een gezondheidszorggebouw met zelfredzame patiënten, danwel bedrijfshulpverleners in een gezondheidszorggebouw met niet-zelfredzame patiënten kan als volgt plaatsvinden:

1 Zonder technische hulpmiddelen

Het alarmeren kan in kleine gezondheidszorggebouwen tijdig geschieden door aanroepen.

2 Met technische hulpmiddelen

Het alarmeren met technische hulpmiddelen kan geschieden door:

- handmatige bediening van communicatiemiddelen
- automatische activering van communicatiemiddelen.

3 Een combinatie van de mogelijkheden 1 en 2

Het alarmeren kan ook getrapt geschieden. Namelijk door roepen naar een lid van het personeel, waarna deze met technische hulpmiddelen de centraalpost in kennis stelt.

4.4.4 Het tijdig

- a ontruimen van een gezondheidszorggebouw met zelfredzame patiënten
- b redden/ontruimen van personen door bedrijfshulpverleners van een gezondheidszorggebouw met niet-zelfredzame patiënten

In geval van b kan onderscheid worden gemaakt in:

- 1 Het redden van de patiënt(en)
- 2 Het ontruimen van de patiënten en overige aanwezigen.

Van 1 zal sprake zijn wanneer er (een) patiënt(en) aanwezig is/zijn in de ruimte waarin brand uitbreekt en er geen personeel in de ruimte of de onmiddellijke omgeving aanwezig is.

In deze situatie kunnen alleen bedrijfshulpverleners die beschikken over adembescherming optreden.

Van 2 zal sprake zijn wanneer er personeel in de brandruimte of de onmiddellijke omgeving aanwezig is. Ontruiming geschiedt dan in aanvang door het aanwezige personeel. In een later stadium behoren bedrijfshulpverleners deze taak van het personeel over te nemen.

In deze situatie wordt ervan uitgegaan dat het gebruik van adembescherming niet noodzakelijk is.

Overigens dient te worden opgemerkt dat een bedrijfshulpverleningsorganisatie niet gelijk kan worden gesteld aan een bedrijfsbrandweer en dat de bedrijfshulpverleners niet zodanig zijn toegerust dat zij onder gelijke omstandigheden als de brandweer kunnen optreden. Gezien hun opleiding en uitrusting worden zij niet verondersteld een brandende ruimte binnen te gaan om iemand te redden, tenzij de brand zich nog in een zodanig pril stadium bevindt, dat de temperatuur in de ruimte dit toelaat.

16

Bepalende factoren:

1 De tijdsduur waarin personen in met rook gevulde ruimten kunnen verblijven
Veelal gaat de ontwikkeling en verspreiding van rook sneller dan die van vuur, met als gevolg dat er meer letselschade optreedt door rook dan door vuur. Rook is voor mensen een levensbedreigende factor. Derhalve moet zoveel mogelijk worden voorkomen dat mensen rook inademen. Met andere woorden: de tijdsduur, waarin personen in met rook gevulde ruimtes moeten verblijven, moet worden beperkt.

2 Redden uit/ ontruimen van een ruimte

Het tijdig redden uit/ ontruimen van een ruimte is afhankelijk van de volgende factoren:

- de mechanische sterkte van het gebouw met het oog op de mogelijkheid van instorten;
- de grootte van de ruimte (loopafstand naar uitgang);
- het aantal personen en hun toestand;
- het aantal, de breedte, de plaats en de beschikbaarheid van de uitgang(en);
- de mate van brandgevaar (brandvoortplanting en dergelijke);
- de mate van rookproductie;
- de mogelijke plaats van een brand in de ruimte;
- de lichtsterkte in een ruimte;
- de geoefendheid van het personeel;
- de indeling van de ruimte met betrekking tot de vluchtroute.

3 Het bereiken van een veilige plaats

Het tijdig vluchten naar een veilige plaats is afhankelijk van de volgende factoren:

- de mechanische sterkte van het gebouw met het oog op de mogelijkheid van instorten;
- de grootte van het gebouw (loopafstand naar een veilige plaats binnen het gebouw in relatie tot de loopsnelheid);
- het aantal personen en hun toestand;
- het aantal, de breedte en de beschikbaarheid van voldoende veilige vluchtroutes;
- de mate van brandgevaar in de vluchtroutes (brandvoortplanting en dergelijke);
- de mate van rookproductie;
- de mogelijke plaats van een brand in het gebouw;

Antonius ziekenhuis, Sneek
(Wiegerink Architecten, Arnhem)

- de indeling van het gebouw met betrekking tot de vluchtroute (het aantal te passeren deuren);
- de lichtsterkte in de vluchtroutes van het gebouw;
- het al dan niet bekend zijn met de vluchtroutes in het gebouw;
- de aanduiding van de vluchtroutes.

Voor het tijdig redden van de aanwezige(n) zijn bovendien de volgende factoren van invloed:

- de loopafstand tussen de plaats waar de bedrijfshulpverleners zich op het moment van alarmeren bevinden en de brandruimte danwel het bedreigde gebied;
- de aanwezigheid van persoonlijke beschermingsmiddelen voor de bedrijfshulpverleners;
- de opleiding en geoefendheid van de bedrijfshulpverleners in het gebruik van deze middelen;
- de eventuele tijd nodig om adembeschermingsapparatuur om te hangen.

4.4.5 Het blussen van een beginnende brand door bedrijfshulpverleners/ personeel van het gezondheidszorggebouw

Of een beginnende brand door bedrijfshulpverleners/personeel kan worden geblust wordt enerzijds beïnvloed door:

- de omvang en de plaats van de brand;
 - de hoeveelheid rook
- en anderzijds door:
- de aanwezigheid van blusmiddelen;
 - de aanwezigheid van persoonlijke beschermingsmiddelen voor de bedrijfshulpverleners;
 - de geoefendheid van bedrijfshulpverleners in het gebruik van deze middelen;
 - de bekendheid van het personeel met de gebruiksinstructie voor de blusmiddelen.

4.4.6 Het zo snel mogelijk automatisch blussen van brand

Het automatisch blussen van brand kan als volgt plaatsvinden:

- door een automatisch blusinstallatie;
- door een blusinstallatie, die aangestuurd wordt door een brandmeldinstallatie.

4.4.7 Het zo snel mogelijk melden van de brand aan de alarmcentrale van de brandweer

Het melden van brand aan de alarmcentrale van de brandweer kan als volgt plaatsvinden:

1 Rechtstreeks aan de brandweeralarmcentrale

Dit kan op de volgende manieren gebeuren:

- handmatig (bijvoorbeeld telefonisch of met behulp van een handbrandmelder met automatische doormelding);
- automatisch met behulp van een brandbeveiligingsinstallatie met doormelding.

2 Niet rechtstreeks aan de brandweeralarmcentrale

Dit kan gebeuren via een andere meldkamer (bijvoorbeeld 06-11-centrale of een particuliere alarmcentrale):

- handmatig (bijvoorbeeld telefonisch of met behulp van een handbrandmelder met automatische doormelding);
- automatisch met behulp van een brandbeveiligingsinstallatie met doormelding.

4.4.8 Het zo snel mogelijk opkomen van de brandweer

Het opkomen van de brandweer (opkomsttijd) wordt bepaald door:

1 De tijd, die nodig is om de brandmelding te verwerken op de alarmcentrale van de brandweer en de desbetreffende brandweereenheid te alarmeren (verwerkingstijd)

Deze tijd is afhankelijk van de mate, waarin de meldingen op de brandweer-alarmcentrale geautomatiseerd kunnen worden verwerkt.

2 De tijd, die de brandweereenheid na alarmering nodig heeft om het brandweervoertuig te bezetten (uitruktijd)

Deze tijd is afhankelijk van de organisatievorm van de brandweer (gekazerneerd of niet gekazerneerd).

3 De tijd die de brandweereenheid na bezetting van het brandweervoertuig nodig heeft om de plaats van de brand te bereiken (rijtijd)

De rijtijd is afhankelijk van de volgende factoren:

- de bekendheid met de te volgen route;
- de afstand tussen brandweerkazeme en de plaats van de brand;
- verkeersbelemmeringen (wegopbrekingen, bruggen, spoorwegen, uitneembare paaltjes, hekken, foutief geparkeerde auto's en dergelijke);
- de status van de wegen tussen brandweerkazeme en de plaats van de brand (doorgaande weg, woonerf en dergelijke);
- de weersgesteldheid (regen, sneeuw, mist en dergelijke);
- de gelijktijdigheid van verschillende meldingen in combinatie met het aantal brandweereenheden in een brandweerkazeme (hierdoor zal wellicht een brandweereenheid van een verderweg gelegen brandweerkazeme moeten worden gealarmeerd).

4.4.9 Het zo snel en adequaat mogelijk inzetten van de brandweer

Het snel en adequaat inzetten van de brandweer wordt bepaald door:

1 De opstelplaats van de brandweereenheid ten opzichte van de plaats van de brand in het gezondheidszorggebouw

Hierbij spelen de volgende factoren een rol:

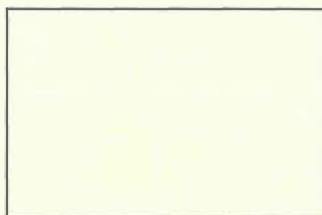
- het aantal opstelplaatsen in relatie tot het aantal toegangen tot het gezondheidszorggebouw;
- de afstand van een opstelplaats tot een toegang van het gezondheidszorggebouw;
- de bekendheid van het brandweerpersoneel met het gezondheidszorggebouw en zijn omgeving met betrekking tot een juiste keuze van opstelplaats en toegang.

2 De mogelijkheid voor brandweerpersoneel om zonder onnodig gevaar voor leven/gezondheid op te kunnen treden in gezondheidszorggebouwen

De mogelijkheid om zonder onnodig gevaar voor eigen leven/gezondheid op te kunnen treden in gezondheidszorggebouwen wordt beïnvloed door:

- de mechanische sterkte van het gebouw met het oog op de mogelijkheid van instorten;
- de mogelijkheid van een goede (radio)communicatie tussen brandweerpersoneel in het gebouw en de bevelvoering buiten het gebouw;
- de bekendheid van het brandweerpersoneel met het gezondheidszorggebouw;
- de gidsfunctie van de bedrijfshulpverleners.

3 Het bereiken van de door brand bedreigde personen en/of de plaats van de brand



Bestuderen van gebouwindeling

Het snel bereiken van de door brand bedreigde personen en/of de plaats van de brand is afhankelijk van:

- het aantal en de plaats van de aanvalswegen;
- de toegankelijkheid van de aanvalswegen (op slot zijnde deuren en dergelijke);
- de mate van vrijwaring tegen rook en vuur van de aanvalswegen;
- de lengte van de aanvalsweg (onder andere hoogte en diepte van het gezondheidszorggebouw);
- de bekendheid met de indeling van het gebouw.

4 Het aansluiten van de brandweereenheid op een bluswatervoorziening

Bij het snel aansluiten van de brandweereenheid op een bluswatervoorziening spelen de volgende factoren een rol:

- de bekendheid met de plaatsen van de bluswatervoorziening;
- de afstand tussen de opstelplaats en de bluswatervoorziening;
- belemmeringen tussen de opstelplaats en de bluswatervoorziening (hek, sloot, beplanting en dergelijke);
- de bereikbaarheid alsmede de beschikbaarheid van de bluswatervoorziening:
 - ondergrondse brandkraan (vastgevroren deksel, geparkeerde auto's, sneeuw, begroeiing en dergelijke);
 - bovengrondse brandkraan (begroeiing, vandalisme en dergelijke);
 - open water, geboorde put en dergelijke (bevroren, zuighoogte en dergelijke).

4.4.10 Het zo snel mogelijk in veiligheid brengen van personen, die zich nog in het bedreigde gebied bevinden

Voor het in veiligheid brengen van personen die zich nog in het bedreigde gebied bevinden spelen de factoren van de hiervoor, onder subparagraaf 4.4.9 beschreven delen 1, 2 en 3, een rol.

4.4.11 Het zo snel en adequaat mogelijk blussen van de brand

In het normatief brandverloop (zie paragraaf 4.2) voor gezondheidszorggebouwen met zelfredzame patiënten wordt ervan uitgegaan dat de brandweer de brand binnen 30 minuten, nadat de brandweer operationeel is, onder controle heeft (brand meester). In de gezondheidszorggebouwen met niet-zelfredzame patiënten is deze tijd gesteld op 44 minuten in verband met eventuele vertraging in de blussing als gevolg van redding. Dit houdt in dat de brand bij daadwerkelijke blussing binnen 30 minuten beheersbaar moet zijn.

De beheersbaarheid van de brand is afhankelijk van:

- de vuurbelasting (permanent en/of variabel);
- de omvang van de brand;
- de mate van brandvoortplanting;
- de slagkracht van de brandweer, gemeten naar het aantal stralen (hoeveelheid water, mankracht en geoefendheid) dat de brandweer direct na het operationeel zijn kan inzetten;
- de aanwezigheid van een automatische blusinstallatie;
- de mate van afvoer van rook- en verbrandingsgassen.

4.4.12 Het zo snel en adequaat mogelijk voorzien in nazorg

In het kader van het brandbeveiligingsconcept gezondheidszorggebouwen is de nazorg uitsluitend gericht op het gezondheidszorggebouw als zodanig en met name op de aspecten die te maken hebben met het voorkomen van gevolgschade.

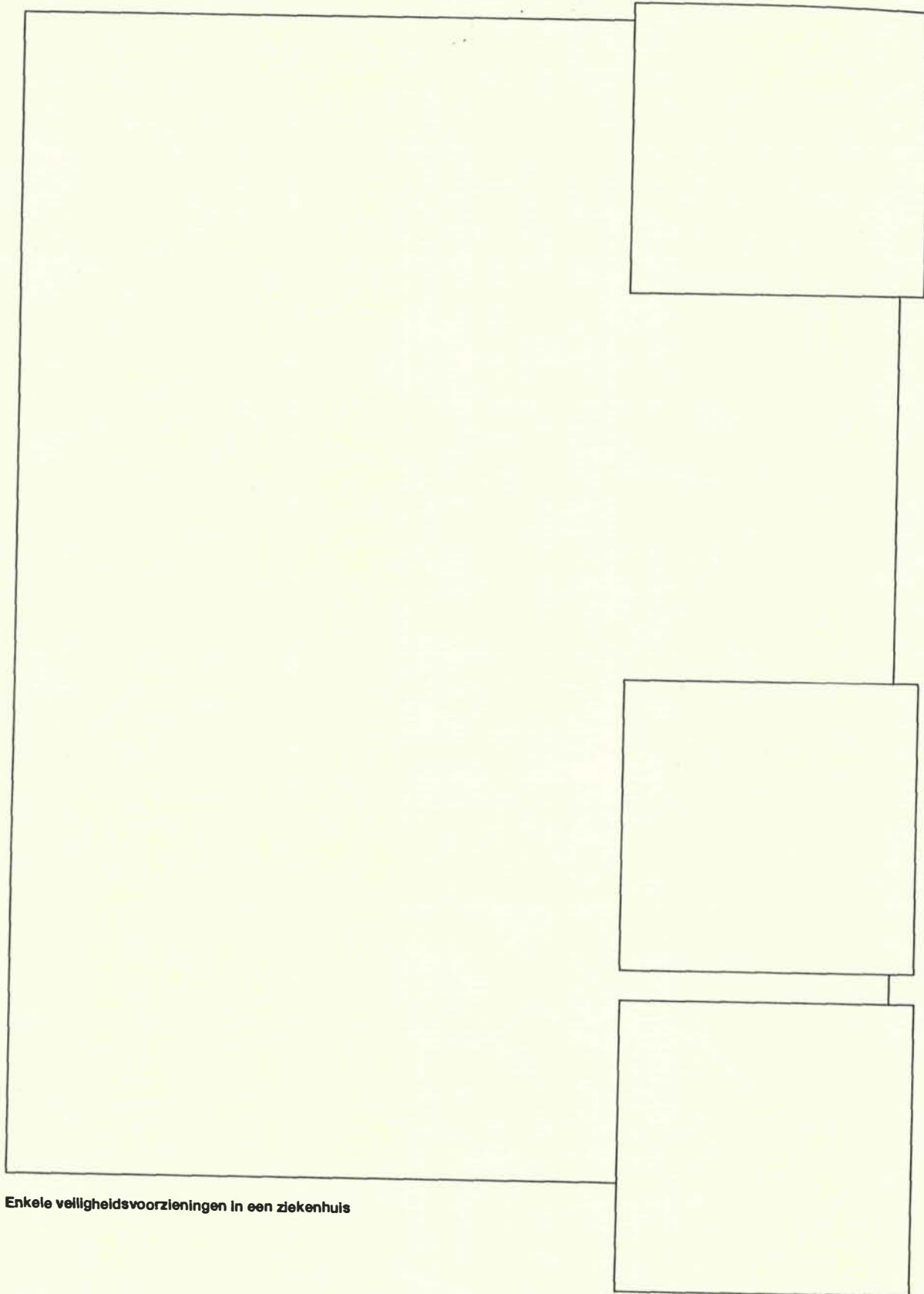
Ter afbakening van het geheel worden de primaire taken van hulpdiensten, overige betrokkenen en de coördinatie hiervan, buiten beschouwing gelaten.

Enkele voorbeelden van primaire taken zijn:

- ambulance-vervoer en/of GGD (slachtofferhulp)
- politie (openbare orde en veiligheid)
- nutsbedrijven (schakelfuncties gas/elektra)
- openbare werken en/of diensten bouw- en woningtoezicht (instortingsgevaar)
- Dienst I-SZW/voorheen Arbeidsinspectie (nader onderzoek in kader Arbowet)
- psychologische opvang getroffen en (voorkoming psychische trauma's).

Bij het zo snel en adequaat mogelijk voorzien in nazorg (het voorkomen van vervolgschade) spelen de volgende factoren een rol:

- het optreden van de brandweer
- het optreden van de gebruiker.



Enkele veiligheidsvoorzieningen in een ziekenhuis

H o o f d s t u k

Brandbeveiligingsmaatregelen

en -voorzieningen op hoofdlijnen

5

Uit de uitgangspunten van het normatief brandverloop (paragraaf 4.2) en de specifieke doelstellingen (paragraaf 4.4) zijn de brandbeveiligingsmaatregelen en -voorzieningen op hoofdlijnen af te leiden.

Deze brandbeveiligingsmaatregelen en -voorzieningen zijn onder te verdelen in de volgende categorieën (aandachtsgebieden):

- planologie
- bouwkunde
- installatie-techniek
- inventaris
- interne organisatie en gebruik
- inzet brandweer.

De bij de betreffende categorie behorende maatregelen en voorzieningen zijn gericht op de brandbeveiliging van gezondheidszorggebouwen als zodanig en dienen geen bredere doelstelling.

Zo wordt hier onder *planologie* verstaan de situering en vorm van de gebouwen in de omgeving, alsmede de ligging van het gebouw ten opzichte van de brandweerkazeme, de bereikbaarheid van het gebouw door de brandweer en de aanwezigheid van een bluswatervoorziening bij het gebouw.

De *bouwkundige* maatregelen en voorzieningen hebben hoofdzakelijk betrekking op de materiaalkeuze van de constructieonderdelen, de stabiliteit van het gebouw – of de onderdelen daarvan – gedurende een brandsituatie, de veilige ontruiming van personen en de beheersbaarheid van een brand.

De *installatie-techniek* spitst zich toe op technische installaties voor de brandbeveiliging van het gebouw als zodanig. Behoudens de reeds genoemde installaties kunnen gezondheidszorggebouwen ook nog andersoortige installaties bevatten. Voorbeelden hiervan zijn luchtbehandelingsinstallaties, liftinstallaties en vanzelfsprekend security-installaties, zoals deurvergrendelingssystemen. Deze installaties hebben in feite niets met de brandbeveiliging te maken en kunnen zelfs de brandveiligheid negatief beïnvloeden. Derhalve zal van dergelijke installaties moeten worden nagegaan of, en zo ja in hoeverre deze installaties op gespannen voet staan met de uitgangspunten en doelstellingen van het brandbeveiligingsconcept. Vervolgens zullen hiervoor doeltreffende oplossingen moeten worden gevonden.

De maatregelen en voorzieningen voor de *inventaris* zijn gericht op inrichtingsgoederen, zoals meubilair, matrassen, beddegoed en dergelijke.

De *interne organisatie en het gebruik* hebben betrekking op het functioneren van een interne organisatie in geval van brand, het brandveilig gebruik van het gebouw als zodanig (bijvoorbeeld vrijhouden van vluchtroutes) en de nazorg.

De *inzet* van de brandweer heeft betrekking op het repressief optreden van de brandweer en de nazorg. De hier te behandelen aspecten van nazorg richten zich in hoofdzaak op het beperken van materiële gevolgschade van een brand.

5.1 Brandbeveiligingsmaatregelen en -voorzieningen voortvloeiend uit de specifieke doelstellingen

Flevoziekenhuis, Almere
Campaman, Tennekes, de Jong Architecten

5.1.1 Het voorkomen van brand

1 Planologie

De situering en de vorm van het gezondheidszorggebouw moeten zodanig zijn dat een optimale sociale controle mogelijk is.

2 Bouwkunde

- De mate van brandbaarheid van de toegepaste constructie-onderdelen moet zodanig worden beperkt, dat de kans op brandvoortplanting, gelet op de bestemming van de ruimte waarin deze constructie-onderdelen worden toegepast, voldoende klein is.
- Materiaal toegepast ter plaatse van of in de nabijheid van een verbrandingstoestel moet zodanig zijn dat, ten gevolge van de in dat materiaal optredende temperatuur veroorzaakt door dat toestel, niet gemakkelijk brand kan ontstaan.
- Materiaal toegepast ter plaatse van of in de nabijheid van een rookkanaal moet zodanig zijn dat, ten gevolge van de in dat materiaal optredende temperatuur als gevolg van het op het kanaal aangesloten toestel, niet gemakkelijk brand kan ontstaan.
- Een dak mag niet zodanig zijn, dat ten gevolge van vliegvlam gemakkelijk brand kan ontstaan.

3 Installatie-techniek

- Energievoorzieningen (gas, elektra) mogen niet gemakkelijk brand veroorzaken.
- Er mogen uitsluitend goedgekeurde technische installaties worden toegepast.
- Voor aanleg van installaties dienen erkende installateurs te worden ingeschakeld.
- Een gezondheidszorggebouw, dat – gezien de omgeving – gevoelig is voor blikseminslag moet daartegen worden beveiligd.

4 Inventaris

- Relatief brandveilige inrichtingsgoederen (meubilair, matrassen, beddegoed en dergelijke) moeten zoveel mogelijk worden toegepast.
- Er mag uitsluitend goedgekeurde apparatuur (KEMA-keur en dergelijke) worden toegepast.
- Er mogen uitsluitend zelfdovende afvalbakken worden toegepast.

5 Interne organisatie en gebruik

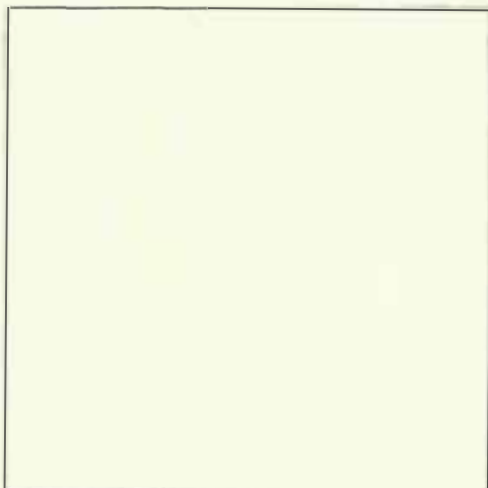
- Op plaatsen met een verhoogd brandrisico moet een rookverbod worden ingesteld.
- Er moet voor worden zorggedragen dat patiënten, waarvan kan worden verwacht dat zij brand willen stichten, geen ontstekingsbronnen (aanstekers, lucifers) in hun bezit hebben of kunnen krijgen.
- Periodieke controles gericht op het voorkomen van brandgevaarlijke situaties moeten worden verricht. Hierbij kan worden gedacht aan:
 - de afstand van verlichtingsspoten tot gordijnen en versiering;
 - het tijdig legen van afvalbakken en dergelijke;
 - het handhaven van orde en netheid in het gezondheidszorggebouw.
- Instructies ten behoeve van het veilig verrichten van brandgevaarlijke werkzaamheden moeten aanwezig zijn en worden nageleefd. Hierbij kan worden gedacht aan lassen, snijbranden, dakdekken en dergelijke.
- Gebruiksvoorschriften moeten worden ingesteld, onder andere ten aanzien van:
 - het uitsluitend inschakelen van erkende installateurs;
 - het verrichten van periodiek onderhoud aan technische installaties en apparatuur;
 - het instrueren van het personeel van het gezondheidszorggebouw ten aanzien van het voorkomen van brand;
 - het vermijden van brandbare buitenopslag en open afvalcontainers.

6 Inzet brandweer

Niet van toepassing.

5.1.2 Het zo snel mogelijk ontdekken van brand

Hier dient onderscheid te worden gemaakt tussen gezondheidszorggebouwen waar uitsluitend of bijna uitsluitend zelfredzame patiënten aanwezig zijn (a) en gezondheidszorggebouwen waar een groot deel, tot alle patiënten niet-zelfredzaam zijn (b).



Beveiligingsvoorzieningen in een ziekenhuis

In geval a blijkt uit het normatief brandverloop dat de ontdekkingstijd wordt gerelateerd aan het moment van vlamoverslag in een brandruimte. Dit is het geval indien er niemand in de brandruimte aanwezig is, of indien er personen in de brandruimte aanwezig zijn, die de brand niet willen melden (brandstichting).

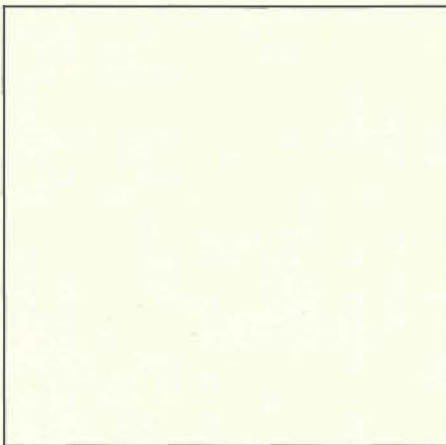
In geval b blijkt uit het normatief brandverloop dat – om te voorkomen dat niet-zelfredzame patiënten in hun bed door verstikking of verbranding omkomen – de ontdekkingstijd wordt gerelateerd aan een brandmeldinstallatie met volledige bewaking.

1 Planologie

Niet van toepassing.

2 Bouwkunde

Niet van toepassing.



Beveiligingsvoorzieningen in een ziekenhuis

3 Installatie-techniek

- In ingewikkelde, afgelegen of hoge gezondheidszorggebouwen waar alleen zelfredzame patiënten aanwezig zijn moet een doeltreffende brandmeldinstallatie met gedeeltelijke bewaking aanwezig zijn.
- In gezondheidszorggebouwen waar overwegend niet-zelfredzame patiënten verblijven moet een doeltreffende brandmeldinstallatie met volledige bewaking aanwezig zijn.

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

Bij het uitvoeren van brandgevaarlijke werkzaamheden dient continu toezicht te worden gehouden door een terzake deskundig persoon.

6 Inzet brandweer

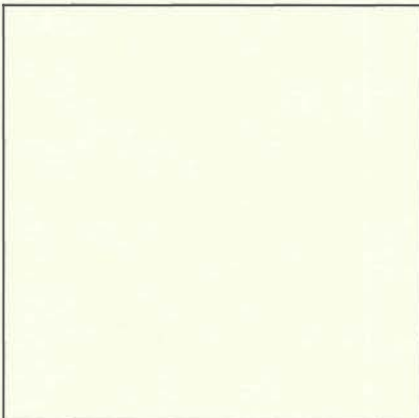
Niet van toepassing.

27

5.1.3 Het zo snel en adequaat mogelijk alarmeren van

- a bedrijfshulpverleners en overige personen in een gezondheidszorggebouw met zelfredzame patiënten
- b bedrijfshulpverleners in een gezondheidszorggebouw met niet-zelfredzame patiënten

De complexiteit of hoogte van een gezondheidszorggebouw met zelfredzame patiënten, alsmede de interne organisatie, bepalen of alarmering met technische hulpmiddelen noodzakelijk is.



- De personen in een gezondheidszorggebouw met zelfredzame patiënten moeten binnen 2 minuten na ontdekking van een brand kunnen zijn gealarmeerd.
- In een gezondheidszorggebouw met niet-zelfredzame patiënten moet een zodanig communicatiesysteem aanwezig zijn, dat de bedrijfshulpverleners zonder tussenkomst van derden worden gewaarschuwd, wanneer de brandmeldinstallatie wordt geactiveerd.
- In een gezondheidszorggebouw met niet-zelfredzame patiënten moeten de bedrijfshulpverleners direct na activering van de brandmeldinstallatie adequaat worden geïnformeerd omtrent de plaats van de brand.

5.1.4 Het tijdig

- a ontruimen van een gezondheidszorggebouw met zelfredzame patiënten
- b redden/ontruimen van personen door de bedrijfshulpverleners van een gezondheidszorggebouw met niet-zelfredzame patiënten

1 Planologie

Niet van toepassing.

2 Bouwkunde

- De hoofdconstructie van een gezondheidszorggebouw behoort zodanig sterk te zijn, dat die constructie bij brand niet binnen een korte tijdsduur instort, opdat de in het gezondheidszorggebouw aanwezige vluchtroutes in stand blijven en door de in het gebouw aanwezige personen, ondanks de brand, kunnen worden gebruikt.

28

Vooralsnog wordt ervan uitgegaan, dat een verblijfsduur van meer dan 30 seconden in een met rook gevulde ruimte ontoelaatbaar is. Gedurende deze tijd is het reëel te veronderstellen dat mensen hun adem kunnen inhouden en lopend een bepaalde afstand door de rook kunnen afleggen. Voor valde personen in gezondheidszorggebouwen kan een loopsnelheid van 1 m/s worden aangehouden. Door rook af te voeren (bijvoorbeeld door een rook- en warmte-afvoerinstallatie) of op te vangen, kan langer over een rookvrije vluchtroute worden beschikt.

Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren teneinde tot een concrete invulling van het bovenvermelde te komen.

Normaliter zullen de op grond van andere eisen de plaats en afmetingen voldoende zijn voor een veilige ontvluchting. Voor specifieke gevallen wordt verwezen naar het betreffende brandbeveiligingsconcept (bijvoorbeeld bij gebruik van een ruimte voor bijeenkomsten zoals kerkdiensten en dergelijke naar het brandbeveiligingsconcept bijeenkomstgebouwen).

- Het gezondheidszorggebouw behoort zodanig in rookcompartimenten te zijn onderverdeeld, dat niet langer dan 30 seconden door de rook hoeft te worden gelopen, dan wel dat bij verplaatsing van niet-zelfredzame patiënten deze niet langer dan 30 seconden in de rook hoeven te verblijven.

- Het aantal uitgangen van een ruimte in een gezondheidszorggebouw, alsmede de breedte en de plaats van de uitgang(en) en de totale breedte van de te gebruiken uitgangen behoren te worden afgestemd op het aantal mogelijk in deze ruimte aanwezige personen, het gebruik van rolstoelen en bedden voor vervoer van niet-zelfredzame patiënten, alsmede de mate van brandgevaar in die ruimte.
- Zelfredzame patiënten, personeel en bezoekers in een gezondheidszorggebouw behoren in beginsel vanuit een verpleegkamer of een andere ruimte via twee richtingen (vluchtroutes) rechtstreeks of uitsluitend via vloeren, trappen en hellingbanen het aansluitende terrein te kunnen bereiken.

Flevozekehuys, Almere
Campaman, Tennekes, de Jong Architecten

Daar er van wordt uitgegaan dat bedgebonden patiënten alleen horizontaal worden verplaatst, zullen in het geval dat een brandcompartiment slechts aan één zijde door een ander brandcompartiment wordt begrensd de patiënten slechts in één richting kunnen worden verplaatst.

Normaliter zullen de op grond van andere elsen de plaats en afmetingen voldoende zijn voor een veilige ontvluchting.

Voor specifieke gevallen wordt verwezen naar het betreffende brandbeveiligingsconcept.

Of een deur niet tegen de vluchtrichting in mag draaien, wordt bepaald door het aantal personen dat van de deur gebruik moet maken.

Speciale aandacht is nodig voor het beperken van de rookproductie van matrassen en beddegoed.

Hierbij kan worden gedacht aan:

- opleiding, voorlichting;
- periodeke oefeningen, al dan niet in samenwerking met de plaatselijke brandweer.

- Niet-zelfredzame patiënten in een gezondheidszorggebouw behoren in beginsel vanuit een verpleegkamer of een andere ruimte via twee richtingen (vluchtroutes) rechtstreeks of uitsluitend via vloeren en hellingbanen naar een veilige plaats te worden gebracht.

- Het aantal vluchtroutes en de situering ervan in een gezondheidszorggebouw, de plaats van de uitgang(en) en de breedte van de vluchtroutes en uitgangen behoren te worden afgestemd op het aantal personen dat er 'gelijktijdig' gebruik van maakt, het gebruik van rolstoelen en bedden voor vervoer van niet-zelfredzame patiënten, alsmede de mate van brandgevaar in het gebouw.

- De in het gezondheidszorggebouw toegepaste constructiematerialen mogen niet in belangrijke mate bijdragen tot de ontwikkeling van de brand en het ontstaan van rook.
- Deuren in een vluchtroute moeten zonder gebruikmaking van een sleutel of een ander los voorwerp kunnen worden geopend en mogen in principe niet tegen de vluchtrichting indraaien.
- Het gezondheidszorggebouw moet worden voorzien van doeltreffende vluchtroute-aanduidingen.
- Personen in een gezondheidszorggebouw mogen bij het ontruimen van het gebouw geen hinder ondervinden van vallend glas ten gevolge van vlamoverslag.

3 Installatie-techniek

Het gezondheidszorggebouw moet worden voorzien van een doeltreffende verlichtingsinstallatie.

4 Inventaris

De in het gezondheidszorggebouw toegepaste inrichtingsmaterialen mogen niet in belangrijke mate bijdragen tot de ontwikkeling van de brand en het ontstaan van rook.

5 Interne organisatie en gebruik

- Er dient een doeltreffend ontruimingsplan aanwezig te zijn, dat is afgestemd op het inzetplan van de brandweer.
- Er dient regelmatig volgens dit ontruimingsplan te worden geoefend.
- De bedrijfshulpverleners dienen zich te allen tijde op een zodanige plaats binnen de inrichting te bevinden dat minimaal 2 van hen binnen 2 minuten elke ruimte waarin zich niet-zelfredzame patiënten bevinden kunnen bereiken.
- De bedrijfshulpverleners en het overige personeel behoren te weten wat ze in geval van brand te wachten staat.

Hierbij kan worden gedacht aan:

- persoonlijke beschermingsmiddelen voor de ademhalingswegen tegen rook, CO en andere giftige gassen;
- voldoende opleiding, oefening en training in het gebruik van de beschermingsmiddelen.

Met name dient te worden voorkomen dat de inzet van de brandweer de ontruiming van het gezondheidszorggebouw stagneert.

- De bedrijfshulpverleners in gezondheidszorggebouwen met niet-zelfredzame patiënten behoren onder minder goede omstandigheden op te kunnen treden.

- De vluchtroutes behoren te worden vrijgehouden.

6 Inzet brandweer

Het inzetplan van de brandweer moet zijn afgestemd op het ontruimingsplan van het gezondheidszorggebouw.

30

5.1.5 Het blussen van een beginnende brand door bedrijfshulpverleners/ personeel van een gezondheidszorggebouw

1 Planologie

Niet van toepassing.

2 Bouwkunde

Niet van toepassing.

3 Installatie-techniek

In het gezondheidszorggebouw behoren doeltreffende brandslanghaspels aanwezig te zijn.

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

- De bedrijfshulpverleners dienen geoefend te zijn in het gebruik van de aanwezige blusmiddelen.
- Overige personeelsleden dienen op de hoogte te zijn van de gebruiksinstructie van de blusmiddelen.
- Voor specifieke situaties (onder andere laboratoriumproeven) dienen doeltreffende draagbare blustoestellen aanwezig te zijn.

6 Inzet brandweer

Niet van toepassing.

5.1.6 Het zo snel mogelijk automatisch blussen van brand

Niet van toepassing.

5.1.7 Het zo snel mogelijk melden van de brand aan de alarmcentrale van de brandweer

1 Planologie

Niet van toepassing.

2 Bouwkunde

Niet van toepassing.

Training ziekenhuispersoneel

3 Installatie-techniek

- In het gezondheidszorggebouw behoort een voorziening (minimaal één telefoontoestel) aanwezig te zijn, waarmee zo snel mogelijk (vanuit een centrale plek) een interne melding van brand aan de 06-11-centrale of de brandweer-alarmsentrale (zonder bijvoorbeeld de tussenkomst van een telefonist(e)) gemeld kan worden.
- Er wordt van uitgegaan dat brandmeldinstallaties en automatische brandblusinstallaties rechtstreeks doormelden aan de brandweeralarmsentrale.

4 Inventaris

Niet van toepassing.

De 06-11-centrale is een doorschakelpost.

Twee gegevens zijn noodzakelijk en voldoende, namelijk 'brandweer' en plaatsnaam om doorverbonden te worden met de juiste brandweer-alarmsentrale. Aan deze laatste centrale moet worden verteld waar en wat er aan de hand is.

Hierbij kan gedacht worden aan het verder integreren van de bestaande afzonderlijke meldkamers (de 06-11-centrale als centrale Ingang, de meldkamers voor politie en ambulance, alsmede de brandweer-alarmsentrale). Bovendien is afstemming tussen de hulpdiensten nodig om vage meldingen doeltreffend af te handelen. Het is noodzakelijk de kwaliteit (snelheid, doeltreffendheid en capaciteit) van de relevante meldkamers/alarmsentrale structureel te bewaken en zo mogelijk te verbeteren.

5 Interne organisatie en gebruik

- Regelmatige(r) voorlichting over de werking van de 06-11-centrale of de brandweeralarmsentrale is noodzakelijk.
- Er wordt van uitgegaan dat de interne organisatie in een gezondheidszorggebouw zodanig is ingericht, dat een brand binnen twee minuten na ontdekking aan de 06-11-centrale of de brandweeralarmsentrale wordt gemeld.

6 Inzet brandweer

De interne en onderlinge organisatie van bij brandmeldingen betrokken meldkamers/alarmsentrales behoren gericht te zijn op optimale snelheid en informatie-inwinning.

Alarmsentrale

31

5.1.8 Het zo snel mogelijk opkomen van de brandweer

1 Planologie

- Er wordt van uitgegaan, dat de locatie van de brandweerkazeme(s) zodanig is dat gezondheidszorggebouwen in het verzorgingsgebied van deze kazeme(s) binnen 8 minuten kunnen worden bereikt.
- Permanente aandacht is nodig voor de verkeers-infrastructuur. Er moet worden gezocht naar oplossingen die zowel de algemene verkeersveiligheid als de snelle brandweeropkomst dienen.

2 Bouwkunde

Niet van toepassing.

3 Installatie-techniek

- Er wordt van uitgegaan, dat de brandweer-alarmcentrale de brandmelding snel en doeltreffend verwerkt. Dat wil zeggen dat binnen 2 minuten na de eerste melding een brandweereenheid is gealarmeerd.
- Bij de uitrit en op hoofdroutes van een brandweerpost zijn soms directe beïnvloedingsmogelijkheden van het verkeer noodzakelijk.

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

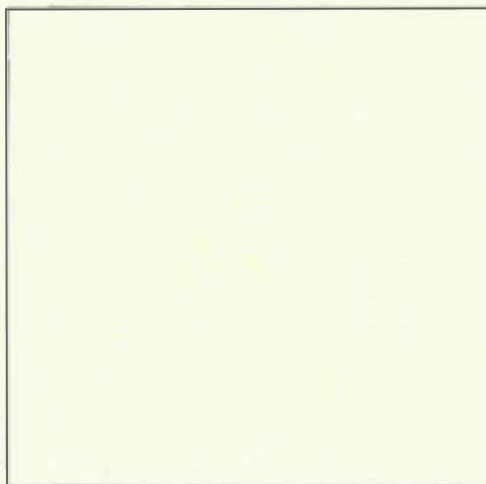
- Er wordt van uitgegaan dat de brandweer binnen vier minuten na alarmering uitrukt.
- Er wordt van uitgegaan dat de brandweer-alarmcentrale beschikt over een doeltreffende alarmregeling, zodat bij afwezigheid van de als eerste in aanmerking komende brandweereenheid de juiste tweede brandweereenheid kan worden gealarmeerd.

6 Inzet brandweer

Niet van toepassing.

32

In bijzondere gevallen, zoals permanent drukke kruispunten met verkeerslichten, kunnen brandweer-voertuigen worden uitgerust met een middel om die lichten te beïnvloeden.



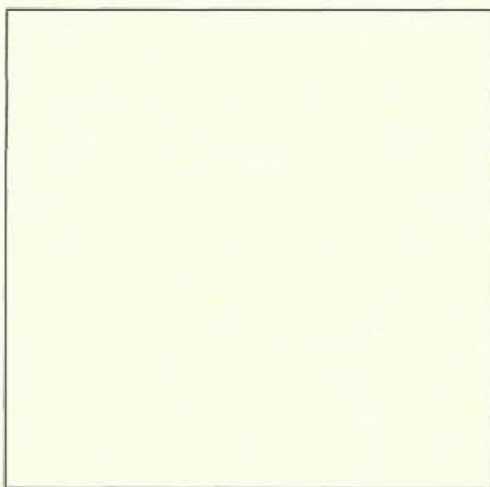
5.1.9 Het zo snel en adequaat mogelijk inzetten van de brandweer

Bij het bepalen van onderstaande maatregelen en voorzieningen is uitgegaan van het landelijk aflegsysteem, namelijk het aflegsysteem lage druk met gebruikmaking van een verdeelstuk (brandwacht, module repressie). Globaal houdt dit aflegsysteem in dat een brandweereenheid bestaande uit 6 personen volgens een vast stramien een brand bestrijdt. De bevelvoerder van de brandweereenheid voert een verkenning uit. Indien redding van personen uit het gezondheidszorggebouw niet noodzakelijk is, kunnen twee personen van de eerste brandweereenheid (de aanvalsploeg) de 1e straal afleggen. Gelijktijdig verzorgen de drie overige personen van deze brandweereenheid (de pompbediener en de waterploeg) eerst de verbinding tussen waterwinplaats en de pomp in het brandweervoertuig en vervolgens bouwen zij vanaf het brandweervoertuig de toevoersleiding naar het verdeelstuk (bij de brandweeringang van het gezondheidszorggebouw) op. Daarna gaat één persoon (de pompbediener) de pomp

van het voertuig bedienen en kan de waterploeg de 2e straal afleggen. Uitgaande van een inzetijd van 7 minuten en een transporttijd van het water van waterwinplaats naar straalpijp van 1 minuut, resteren er voor de waterploeg 6 minuten om een verbinding tussen waterwinplaats en verdeelstuk te realiseren. De aanvalsploeg heeft maximaal 7 minuten om een straal af te leggen vanaf het verdeelstuk tot bij de brand.

De complexiteit en de aard van een gezondheidszorggebouw bepalen in belangrijke mate het aantal (nood)uitgangen. Elke (nood)uitgang is tegelijkertijd een toegang. Daar van te voren niet bekend is, waar een eventuele brand zich voordoet, kan elke toegang de toegang zijn, die zich het dichtst bij de brand bevindt.

Het ministerie van Binnenlandse zaken heeft opdracht gegeven tot een onderzoek naar de beheersbaarheid van brand. Hierbij komt tevens de bluswaterbehoefte aan de orde.



In de praktijk betekent dit dat de vluchtroutes tevens de aanvalswegen zijn.

Daar van te voren niet bekend is, waar een eventuele brand zich voordoet, kan elke vluchtroute als aanvalsweg dienen. Dit betekent dat trappenhuisen waardoor een vluchtroute voert gedurende bedoelde tijd van brand zijn vrijwaard.

1 Planologie

- Er wordt van uitgegaan, dat vanaf een opstelplaats binnen drie minuten na aankomst op deze opstelplaats een slangleiding tot de toegang van het gezondheidszorggebouw, die zich het dichtst bij de brand bevindt, kan worden opgebouwd.
- Er wordt van uitgegaan, dat de eerste brandweereenheid binnen drie minuten na aankomst op de opstelplaats kan zijn aangesloten op een bluswatervoorziening met een nog nader te bepalen capaciteit en gebruiksduur.

2 Bouwkunde

- Poorten en onderdoorgangen, die van belang zijn voor het benaderen van het gezondheidszorggebouw met een brandweervoertuig, behoren te voldoen aan de normale maatvoering van dergelijke passages op de openbare weg.
- De hoofddraagconstructie van een gezondheidszorggebouw behoort zodanig sterk te zijn, dat die constructie bij brand niet binnen een bepaalde tijdsduur instort, opdat de in het gezondheidszorggebouw aanwezige aanvalswegen in stand blijven en door de brandweer, ondanks de brand, kunnen worden gebruikt.
- Voor de aanvalswegen in een gezondheidszorggebouw behoren de in subparagraaf 5.1.4 gestelde bouwkundige voorzieningen te zijn getroffen.
- Indien een trappenhuis deel uit maakt van een aanvalsweg, behoort dit trappenhuis gedurende de tijd dat de brandweer er voor de blussing gebruik van maakt van brand te zijn vrijwaard.
- Ruimten, waarin zich gevaarlijke stoffen bevinden (bijvoorbeeld radio-actieve stoffen), die bij brand, vanwege het gevaarsaspect (in voorbeeld straling) niet door de brandweer kunnen worden bestreden, moeten brandwerend worden omsloten. Deze brandwerendheid (in minuten) moet minimaal de in de ruimten en in de omgeving aanwezige vuurbelasting (kg vurehout per m²) bedragen.

Doorgaans volstaan daartoe de eigen communicatie-middelen van de brandweer. Wanneer die in een bepaald gebouw of bouwwerk onvoldoende werken, dient in dat gebouw of bouwwerk een voorziening te worden getroffen, die het beoogde effect heeft op de werking van de gebruikelijke communicatiemiddelen.

3 Installatie-techniek

In en om gezondheidszorggebouwen behoort een goede (radio)communicatie tussen brandweereenheden verzekerd te zijn.

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

- Er wordt ervan uitgegaan dat voor complexe of hoge gezondheidszorggebouwen de brandweer beschikt over een doeltreffend aanvalsplan.
- Er wordt ervan uitgegaan dat de brandweer kan beschikken over vrijgehouden opstelplaatsen.
- Er wordt van uitgegaan dat, indien in het gebouw geen personen aanwezig zijn, de brandweer zich toegang moet kunnen verschaffen tot het gezondheidszorggebouw zonder schade aan te richten.
- Er wordt van uitgegaan dat, indien in het gebouw personen aanwezig zijn, de interne organisatie zodanig is ingericht, dat de brandweer bij aankomst wordt opgevangen en wordt voorzien van relevante informatie.
- Er wordt van uitgegaan dat de brandweer de deuren in aanvalswegen moet kunnen openen zonder schade aan te brengen.

34



Aanvalsplan, gem. brandweer Rotterdam

6 Inzet brandweer

Er wordt ervan uitgegaan dat de brandweer beschikt over een doeltreffend inzetplan.

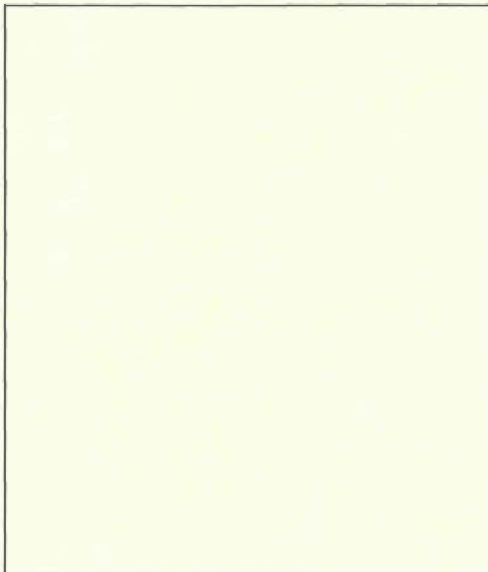
5.1.10 Het zo snel en adequaat mogelijk in veiligheid brengen van personen, die zich nog in het bedreigde gebied bevinden

1 Planologie

Niet van toepassing.

In de praktijk betekent dit dat de vluchtroutes tevens de aanvalswegen zijn.

Daar van te voren niet bekend is, waar een eventuele brand zich voordoet, kan elke vluchtroute als aanvalsweg dienen. Dit betekent dat trappehuizen waardoor een vluchtroute voert gedurende bedoelde tijd van brand zijn gevrijwaard.



Nooduitgang

De bepaling van de grootte van een brand-compartiment hangt af van vele factoren, waaronder:

- de vuurbelasting;
- de omvang van de brand;
- de mate van brandvoortplanting;
- de slagkracht van de brandweer.

Op grond van de 'handleiding Brandweezorg' wordt bij gezondheidszorggebouwen de inzet voor brandbestrijding van één brandweereenheid voldoende geacht.

De hoeveelheid bluswater waarover deze eenheid dient te beschikken is onderwerp van een onderzoek waarvoor het ministerie van Binnenlandse Zaken opdracht heeft gegeven;

- mate van brandbaarheid van de constructiedelen;
- de aanwezigheid van een automatische blusinstallatie;
- de mate van afvoer van rook- en verbrandingsgassen.

Het ministerie van Binnenlandse Zaken heeft opdracht gegeven een onderzoek in te stellen naar de beheersbaarheid van brand.

In de praktijk betekent dit dat de vluchtroutes tevens de aanvalswegen zijn.

2 Bouwkunde

- Voor de aanvalswegen in een gezondheidszorggebouw behoren de in subparagraaf 5.1.4 gestelde bouwkundige voorzieningen te zijn getroffen.
- Indien een trappenhuis deel uitmaakt van een aanvalsweg, behoort dit trappenhuis gedurende de tijd dat de brandweer er voor de blussing gebruik van maakt van brand te zijn gevrijwaard.

3 Installatie-techniek

Niet van toepassing

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

Niet van toepassing.

6 Inzet brandweer

Er wordt van uitgegaan dat de brandweer beschikt over een doeltreffend inzetplan.

5.1.11 Het zo snel en adequaat mogelijk blussen van de brand

1 Planologie

Niet van toepassing.

2 Bouwkunde

- Het gezondheidszorggebouw behoort zodanig in brandcompartimenten te zijn verdeeld, dat de brandweer in staat is een brand in een brandcompartiment binnen 60 minuten na het ontstaan onder controle te krijgen.

- Voor de aanvalswegen in een gezondheidszorggebouw behoren de in subparagraaf 5.1.4 gestelde bouwkundige voorzieningen te zijn getroffen.

Daar van te voren niet bekend is, waar een eventuele brand zich voordoet, kan elke vluchtroute als aanvalsweg dienen. Dit betekent dat trappehuizen waardoor een vluchtroute voert gedurende bedoelde tijd van brand zijn gevluchtwaard.

■ Indien een trappehuis deel uitmaakt van een aanvalsweg, behoort dit trappehuis gedurende de tijd dat de brandweer er voor de blussing gebruik van maakt van brand te zijn gevluchtwaard.

3 Installatie-techniek

Niet van toepassing.

4 Inventaris

Niet van toepassing.

5 Interne organisatie en gebruik

Niet van toepassing.

6 Inzet brandweer

Er wordt van uitgegaan dat de brandweer beschikt over een doeltreffend inzetplan.

5.1.12 Het zo snel en adequaat mogelijk voorzien in nazorg (het voorkomen van vervolgschade)

1 Planologie

Niet van toepassing.

2 Bouwkunde

Niet van toepassing.

3 Installatie-techniek

Niet van toepassing.

4 Inventaris

Niet van toepassing.

Na de bluswerkzaamheden kan in overleg met de beheerder/elgenaar van het gebouw aandacht worden besteed aan verdere schadebeperkende maatregelen.\

De stichting Salvage neemt maatregelen inzake:

- Het zoveel mogelijk beperken van de (gevolg) schade bij en na brand. Dit kan onder andere plaatsvinden door het snel nemen van een aantal betrekkelijke simpele maatregelen opdat zo spoedig mogelijk een zogenaamde corrosiestop wordt bereikt, waarmee verdere schade door verwoestende inwerking van zoutzuur op de niet of slechts gedeeltelijke beschadigde zaken voorkomen kan worden.
- Het met raad en daad terzijde staan van de gedupeerde(n).
- Het in een zo vroeg mogelijk stadium zicht krijgen op de oorzaak en de omvang van de schade.

5 Interne organisatie en gebruik

Er wordt van uitgegaan dat in overleg met de brandweer maatregelen gericht op het in veiligheid brengen van goederen worden genomen.

6 Inzet brandweer

- Er wordt van uitgegaan dat het repressief optreden van de brandweer zodanig is dat zoveel als mogelijk rekening wordt gehouden met het voorkomen van vervolgschade, waaronder rook en/of waterschade.
- Er wordt van uitgegaan dat de brandweer indien nodig de stichting Salvage van de brand op de hoogte stelt.

5.2 Aanvullende brandbeveiligingsmaatregelen en -voorzieningen

Indien in een gezondheidszorggebouw, door hoogte of omvang, niet kan worden voldaan aan de in het normatief brandverloop genoemde uitgangspunten betreffende ontruimingstijd en inzetijd, kan het nodig zijn door het treffen van extra maatregelen de ontruimingstijd en/of inzetijd te beïnvloeden.

Deze beïnvloeding moet zodanig zijn dat een veilige ontruiming en beheersbaarheid van brand wordt verzekerd op basis van de doelstellingen van het brandbeveiligingsconcept.

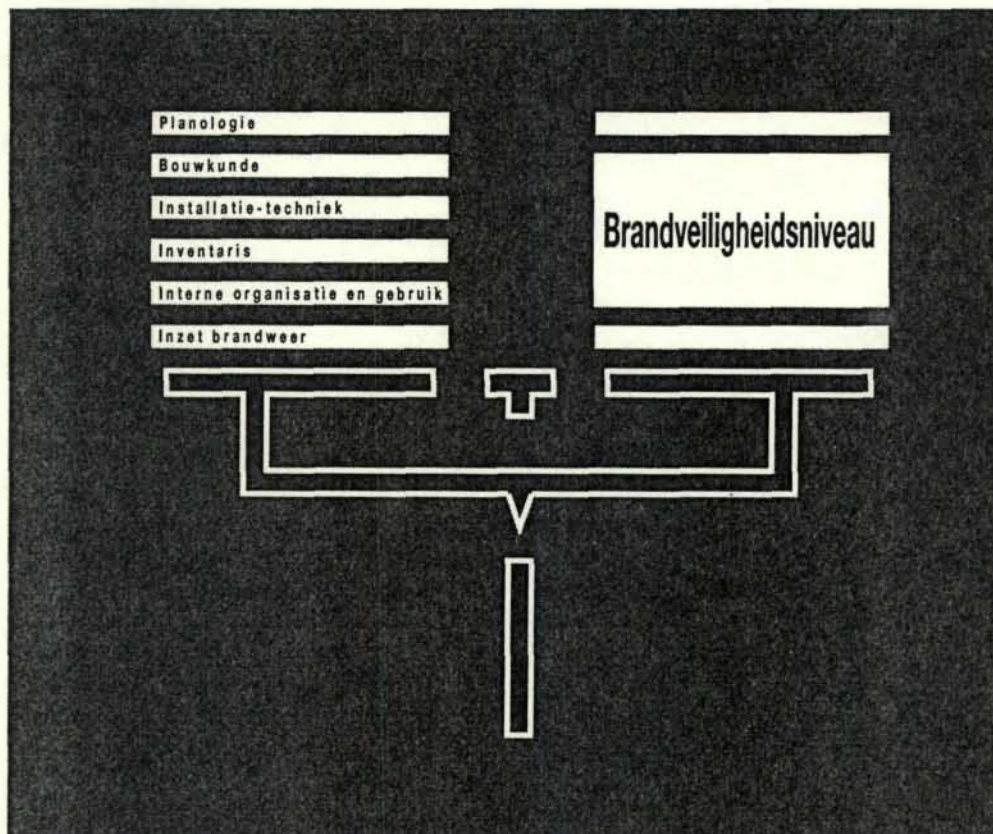
De brandveiligheidsbalans (zie figuur 5.1) laat zien, dat – gegeven het brandveiligheidsniveau – bepaalde maatregelen en voorzieningen uitwisselbaar zijn. De regelgever kan hiervan bij het opstellen van regelgeving gebruik maken.

Zo kan bijvoorbeeld de beschikbare ontruimingstijd in een gebouw met zelfredzame patiënten worden verlengd door het aanbrengen van een brandmeldinstallatie.

Ook is het mogelijk de inzetijd te verkorten door bijvoorbeeld hoge gebouwen van één of meer brandweerliften te voorzien.

37

Figuur 5.1 Brandveiligheidsbalans



5.2.1 Maatregelen die de ontruimingstijd beïnvloeden

In principe kan de ontruimingstijd in gezondheidszorggebouwen met zelfredzame patiënten worden beïnvloed door de volgende maatregelen en voorzieningen:

- De ontruimingstijd kan worden verlengd door beter beveiligde trappehuizen toe te passen.
 - De ontruimingstijd kan worden verlengd door de ontdekkingstijd te bekorten.
- In gezondheidszorggebouwen met niet-zelfredzame patiënten is de ontruimingstijd door bovengenoemde maatregelen niet te beïnvloeden. In deze gezondheidszorggebouwen wordt in principe niet verticaal ontruimd en is een brandmeldinstallatie met volledige bewaking reeds aanwezig.
- Daarnaast kan een (volledige) ontruiming worden voorkomen door de brand vrijwel direct na het ontstaan automatisch te blussen of onder controle te houden (blustijd < 5 minuten).

1 Trappehuizen

Zoals bij de uitgangspunten van het normatief brandverloop voor gezondheidszorggebouwen met zelfredzame patiënten reeds is vermeld, is een trappenhuis gedurende ten minste 30 minuten (dus 15 minuten na alarmering) van grote hoeveelheden rook gevrijwaard. Een trappenhuis moet minimaal 60 minuten van brand zijn gevrijwaard (zie onder andere subparagraaf 5.1.11 Bouwkunde).

De reden dat de waarde voor rookwering lager is, ligt in het feit dat tijdens de ontruiming trappenhuisdeuren worden geopend voor het passeren van personen. Hierdoor kan op de verdieping van de brand rook in het trappenhuis komen.

De brandweer kan met behulp van persluchtapparatuur wel langer dan 30 minuten gebruik blijven maken van het onder de rook staande trappenhuis.

Bij een afdaaltijd per bouwlaag van 1 minuut kan een gezondheidszorggebouw voor zelfredzame personen ongeveer 50 meter hoog zijn. De afdaaltijd is bepalend voor de toelaatbare gebouwhoogte. Indien de afdaaltijd per bouwlaag 2 minuten bedraagt, mag de hoogte van het gezondheidszorggebouw ongeveer 25 meter bedragen.

Gelet op de huidige bouwpraktijk is de afdaaltijd per bouwlaag van 1 minuut een theoretische waarde, omdat de dimensionering van trappehuizen voor de gestelde ontruimingstijd bij hogere gebouwen veelal ontoereikend is.

Een mogelijke oplossing is de gefaseerde ontruiming. Op de verdieping waar de brand woedt moeten dan alle aanwezigen binnen één minuut in het trappenhuis zijn. Op de overige verdiepingen moeten de aanwezigen zich binnen één minuut voor het trappenhuis bevinden. Vervolgens worden de verdiepingen in het gezondheidszorggebouw fasegewijs ontruimd.

Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren ten einde tot een concrete invulling van een gefaseerde ontruiming te komen.

Door de trappehuizen moeilijker rooktoegankelijk te maken, kan de ontruimingstijd en daarmee de hoogte van een gezondheidszorggebouw toenemen.

De ontruimingstijd kan echter niet onbeperkt worden opgerekt. Bij een bepaalde hoogte van het gezondheidszorggebouw dient de vraag te worden gesteld of valide mensen fysiek nog wel in staat kunnen worden geacht veilig het straatniveau te bereiken. Deze hoogte wordt vooralsnog gesteld op 100 meter (zeer hoge gezondheidszorggebouwen). Boven deze hoogte dient de brand zeer snel na het ontstaan automatisch geblust of onder controle te zijn (blustijd < 5 minuten), zodat (algehele) ontruiming niet noodzakelijk is (zie punt 3 van deze paragraaf).

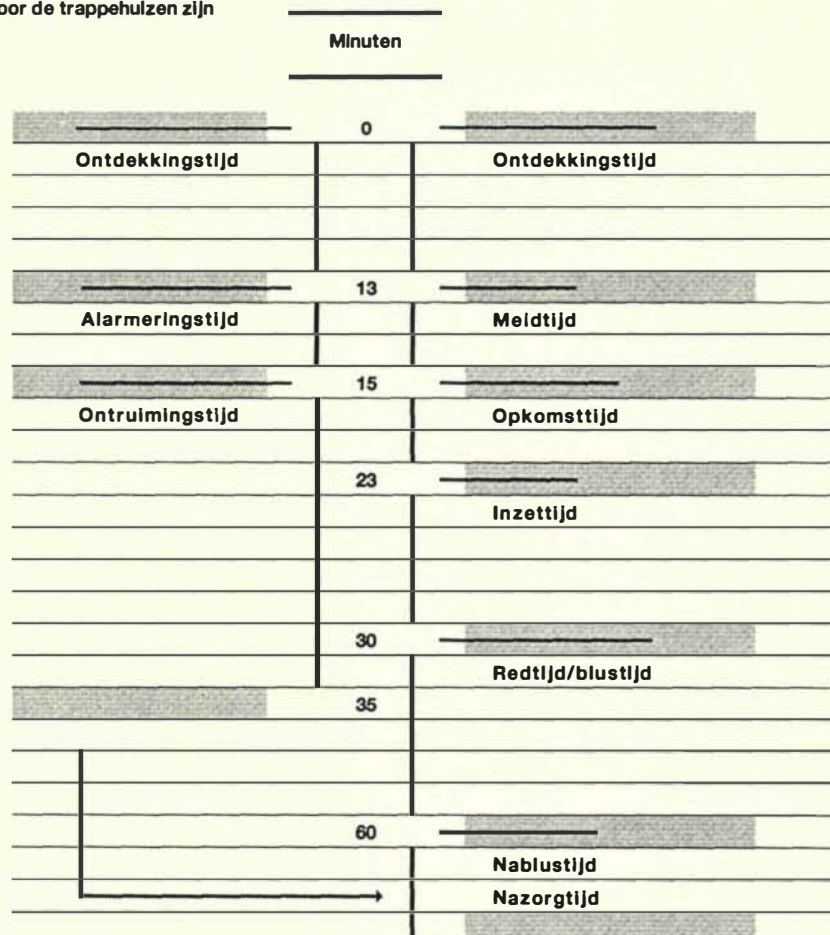
Er zijn verschillende manieren om een trappehuis moeilijker rooktoegankelijk te maken. Namelijk door:

- elke toegang tot het trappehuis te voorzien van een sluis;
- het trappehuis tijdens brand automatisch van overdruk te voorzien, alsmede elke toegang tot het trappehuis te voorzien van een sluis;
- het trappehuis uit te voeren als veiligheidstrappehuis.

Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren ten einde tot een concrete invulling van de hiernaast vermelde voorziening te komen.

1a elke toegang tot het trappehuis te voorzien van een sluis
 Vooralsnog wordt ervan uitgegaan dat een trappehuis met dergelijke voorzieningen gedurende minimaal 35 minuten (dus 20 minuten na alarmering) gevrijwaard zal zijn van grote hoeveelheden rook (zie figuur 5.2). Bij een afdaltijd per bouwlaag van 1 minuut kan een gezondheidszorggebouw met zelfredzame patiënten theoretisch maximaal 66 meter hoog zijn.

Figuur 5.2 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw sluisen voor de trappehuizen zijn aangebracht

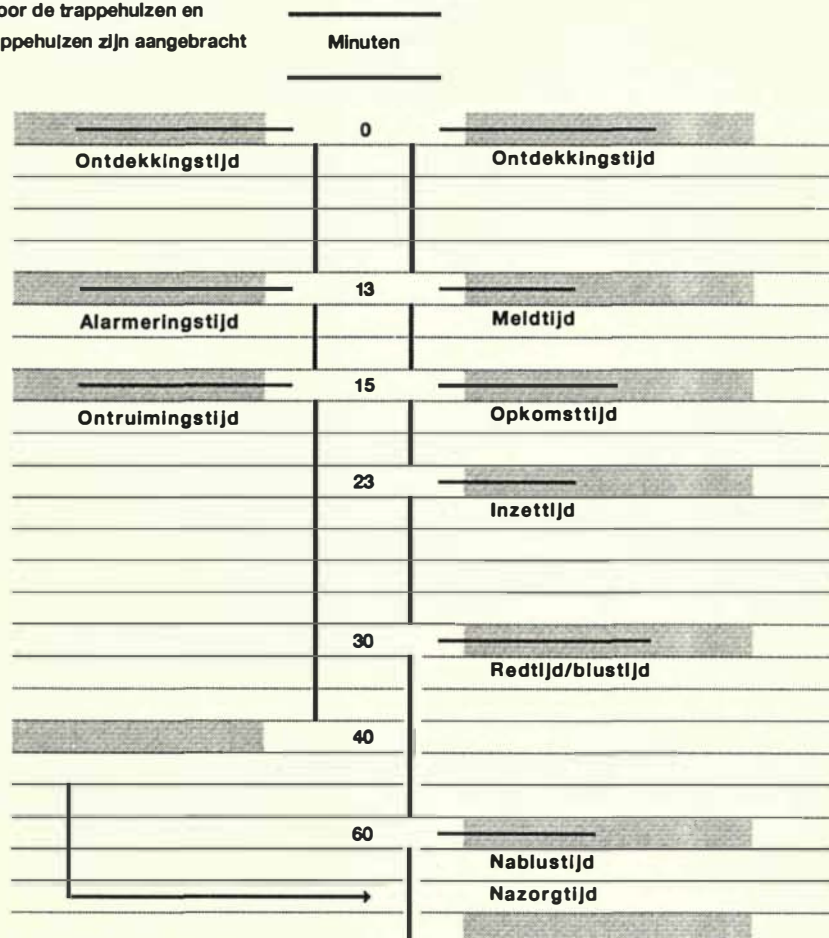


Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren ten einde tot een concrete invulling van de hiernaast vermelde voorziening te komen.

1b het trappenhuis tijdens brand automatisch van overdruk te voorzien, alsmede elke toegang tot het trappenhuis te voorzien van een sluis
Vooralsnog wordt ervan uitgegaan dat een trappenhuis met dergelijke voorzieningen gedurende minimaal 40 minuten (dus 25 minuten na alarmering) gevrijwaard zal zijn van grote hoeveelheden rook (zie figuur 5.3).

Bij een afdaaltijd per bouwlaag van 1 minuut kan een gezondheidszorggebouw met zelfredzame patiënten theoretisch maximaal 83 meter hoog zijn.

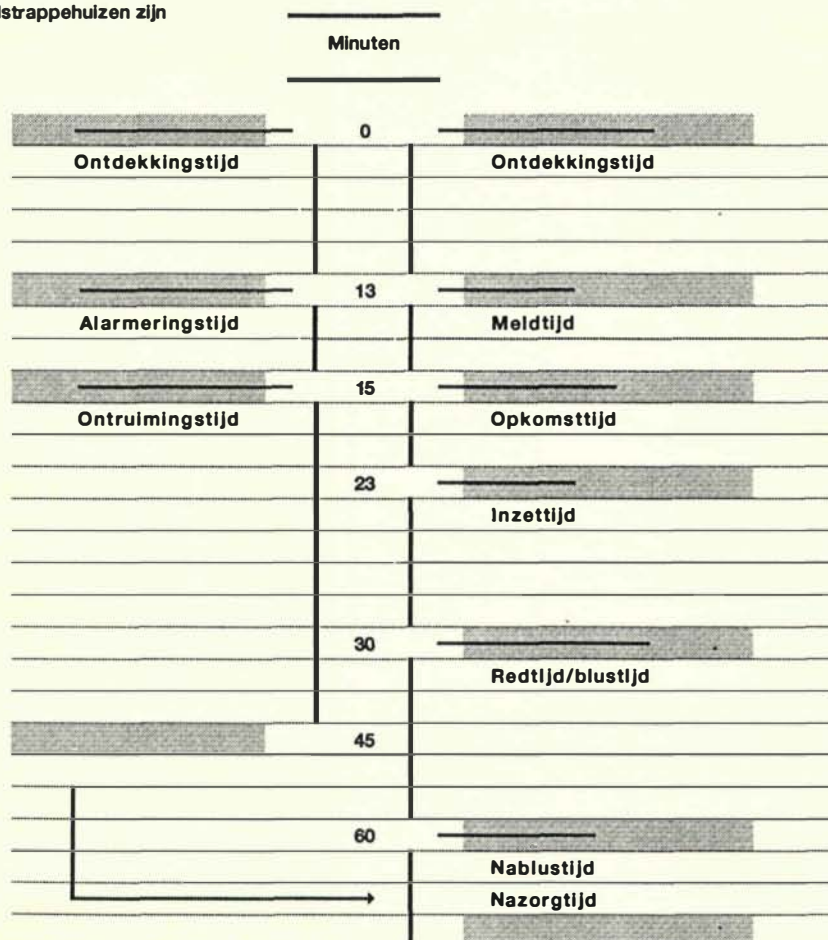
Figuur 5.3 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw sluisen voor de trappenhuis en overdruk in de trappenhuis zijn aangebracht



Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren ten einde tot een concrete invulling van de hiernaast vermelde voorziening te komen.

1c het trappenhuis als veiligheidstrappenhuis uit te voeren
 Vooral nog wordt ervan uitgegaan dat een veiligheidstrappenhuis gedurende minimaal 45 minuten (dus 30 minuten na alarmering) gevrijwaard zal zijn van grote hoeveelheden rook (zie figuur 5.4). Bij een afdaltijd per bouwlaag van 1 minuut kan een gezondheidszorggebouw met zelfredzame patiënten theoretisch maximaal 100 meter hoog zijn.

Figuur 5.4 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw veiligheidstrappenhuisen zijn aangebracht



2 Het bekorten van de ontdekkings tijd

De ontdekkings tijd in gezondheidszorggebouwen met zelfredzame patiënten kan worden bekort door het aanbrengen van een brandmeldinstallatie met volledige bewaking. Door toepassing van een dergelijke installatie kan de ontdekkings tijd tot 5 minuten worden teruggebracht.

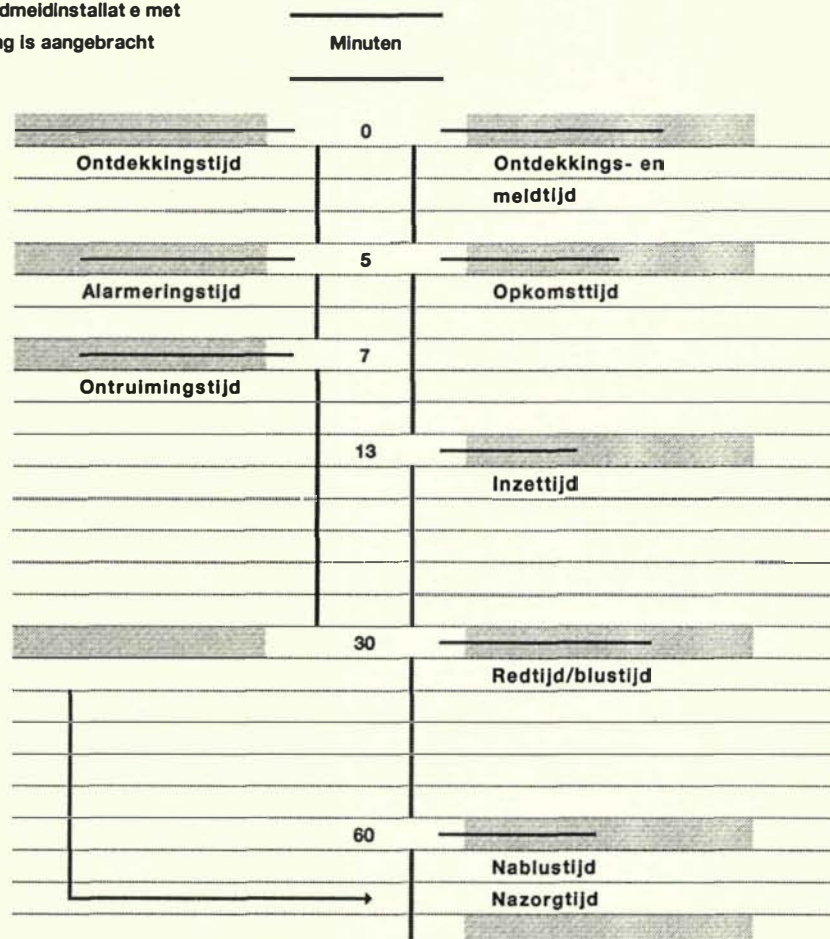
Mede gerekend de tijd nodig voor alarmeren van de aanwezigen kan hierdoor een tijdswinst van ongeveer 8 minuten worden bereikt (zie figuur 5.5).

Bij een afdaaltijd per bouwlaag van 1 minuut kan een gezondheidszorggebouw met zelfredzame patiënten met 'normale' trappehuizen (dus zonder sluis en/of overdruk) en voorzien van een brandmeldinstallatie met volledige bewaking theoretisch maximaal 75 meter hoog zijn.

In tegenstelling tot de aanwezigheid van een brandmeldinstallatie met volledige bewaking in gezondheidszorggebouwen met niet-zelfredzame patiënten is een ontdekkings tijd van 5 minuten aangehouden. Onderzoek heeft aangetoond, dat de automatische ontdekking van brand in een verpleegkamer binnen één minuut plaatsvindt.

In andere ruimten kan automatische ontdekking van brand langer duren. Hierbij wordt een maximum van 5 minuten aangehouden.

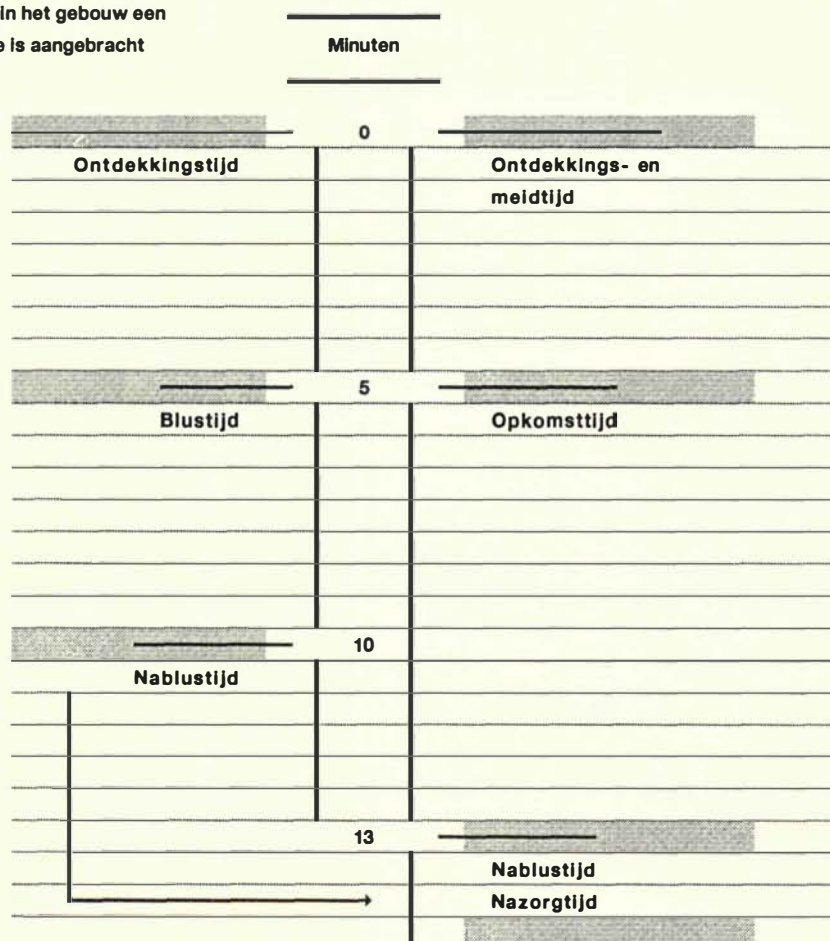
Figuur 5.5 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw een brandmeldinstallatie met volledige bewaking is aangebracht



3 Het voorkomen van ontruiming door de brand vrijwel direct na het ontstaan automatisch te blussen en onder controle te houden (blustijd < 5 minuten)

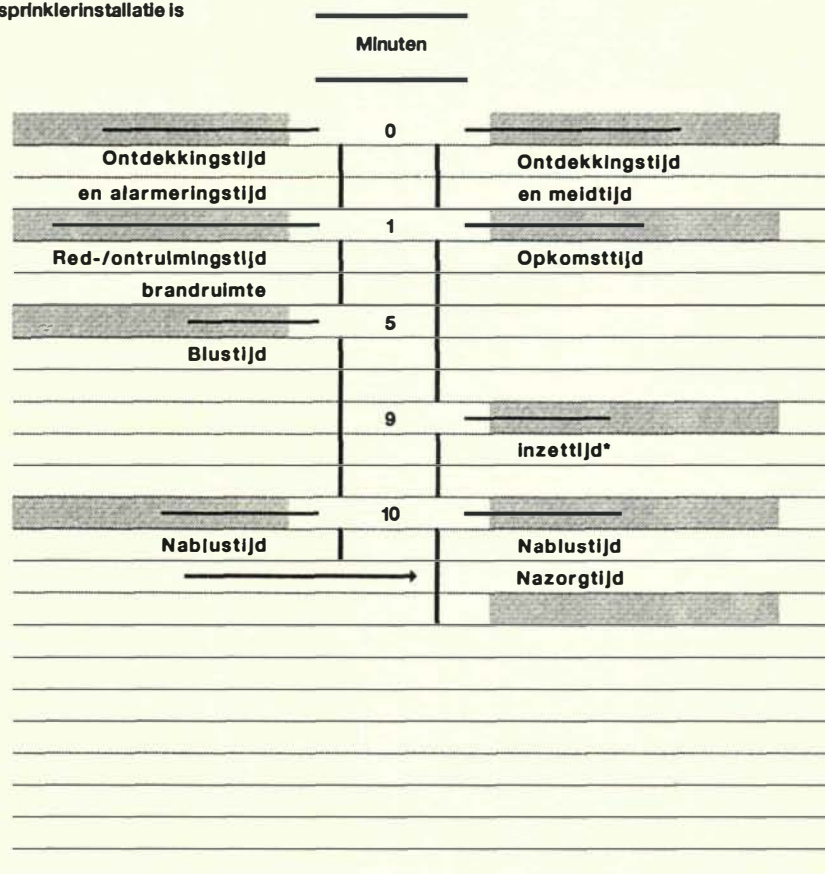
Door het toepassen van een automatische sprinklerinstallatie kan een brand worden geblust of ten minste onder controle worden gehouden. Hierdoor is een volledige ontruiming van een gezondheidszorggebouw met zelfredzame patiënten niet nodig (zie figuur 5.6).

Figuur 5.6 Normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw een sprinklerinstallatie is aangebracht



Het redden/ontruimen van niet-zelfredzame patiënten uit de brandruimte blijft ook met toepassing van een sprinklerinstallatie noodzakelijk.
Op het moment dat de sprinkler aanspreekt (binnen 5 minuten na het ontstaan van de brand) zullen normaliter de niet-zelfredzame patiënten al uit de brandruimte zijn gehaald en in veiligheid zijn gebracht (zie figuur 5.7).

Figuur 5.7 Normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten waarbij in het gebouw een brandmeldinstallatie met volledige bewaking en een sprinklerinstallatie is aangebracht



* brandweer zal bij goede werking sprinkler niet tot een inzet behoeven over te gaan.

5.2.2 Maatregelen en voorzieningen, die de inzet(tijd) beïnvloeden

In principe kan de inzet(tijd) worden beïnvloed door de volgende maatregelen en voorzieningen:

- 1 het treffen van technische voorzieningen die de snelheid van de inzet verhogen, zoals brandweerliften en droge blusleidingen, waardoor de inzet(tijd) wordt verkort
- 2 de ontdekkings(tijd) en meld(tijd) bekorten, waardoor meer tijd beschikbaar is voor de inzet
- 3 de opkomst(tijd) bekorten, waardoor meer tijd beschikbaar is voor de inzet.

Daarnaast kan een brandweerinzet worden voorkomen door de brand vrijwel direct na het ontstaan automatisch te blussen of onder controle te hebben (blustijd < 5 minuten).

1 Het treffen van voorzieningen, die de snelheid van de inzet verhogen

De inzet(tijd) van de brandweer heeft een directe relatie met de hoogte van het gezondheidszorggebouw. In het normatief brandverloop bedraagt de inzet(tijd) 7 minuten. Er van uitgaande dat binnen 1 minuut na aankomst het trappenhuis kan worden bereikt, blijven er voor het bereiken van de verdieping waar de brand woedt 6 minuten over. Uitgaande van het gegeven dat de brandweer met perslucht, slang(en) en eventueel ander materiaal meenemend in een zodanige conditie de verdieping van de brand moet bereiken, dat direct met de vervolgwerkzaamheden kan worden aangevangen, wordt voor het overbruggen van een verdieping voorlopig 1 minuut aangehouden. Dit betekent dat een gezondheidszorggebouw zonder aanvullende brandbeveiligingsvoorzieningen ongeveer 20 meter hoog (6 verdiepingen) kan zijn. Vooralsnog wordt ervan uitgegaan, dat deze hoogte ook de maximale hoogte is die brandweermensen lopend kunnen overbruggen en direct daarna fysiek in staat zijn eventueel mensen in veiligheid te brengen en de brand effectief te blussen.

Met de toepassing van doeltreffende brandweerlift(en) en droge blusleiding(en) kan een hoger gezondheidszorggebouw worden gerealiseerd. Brandweereenheden kunnen water met voldoende druk leveren tot ongeveer 70 meter hoogte. Vanaf die hoogte moeten gezondheidszorggebouwen worden voorzien van blusleiding(en) met een pompinstallatie. In ingewikkelde gebouwen kan zich in het horizontale vlak, vanwege de noodzaak van een snelle inzet, een vergelijkbare situatie voordoen. In dat geval is een droge blusleiding in het horizontale vlak een oplossing.

Het ministerie van Binnenlandse Zaken overweegt onderzoek te initiëren ten einde de maximale hoogte van een gebouw zonder brandweerlift en blusleiding vast te stellen, uitgaande van de fysieke mogelijkheden van het brandweerpersoneel.

2 Het bekorten van de ontdekkings- en meld(tijd)

De inzet(tijd) kan worden verlengd door de ontdekkings- en meld(tijd) te bekorten. Dit kan alleen maar in gezondheidszorggebouwen met zelfredzame patiënten door het toepassen van een doeltreffende brandmeldinstallatie met volledige bewaking. In gezondheidszorggebouwen met niet-zelfredzame patiënten is op grond van andere overwegingen al een doeltreffende brandmeldinstallatie met volledige bewaking noodzakelijk. Door toepassing van een dergelijke installatie kan in gezondheidszorggebouwen met zelfredzame patiënten de ontdekkings(tijd) tot 5 minuten worden bekort. Hierdoor kan een tijdswinst van 10 minuten worden bereikt (zie figuur 5.5).

Gelet op de hiervoor beschreven fysieke mogelijkheden van het brandweerpersoneel is de maximale hoogte voor gezondheidszorggebouwen zonder brandweerlift en blusleiding (ook met langere inzet(tijd)) vooralsnog ongeveer 20 meter.

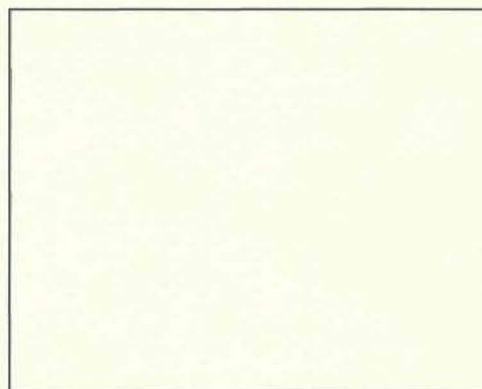
3 Het bekorten van de opkomsttijd

De inzetijd kan worden verlengd door de opkomsttijd te bekorten. Dit kan door de aanwezigheid van een doeltreffende bedrijfsbrandweer. Hierdoor kan de opkomsttijd tot ongeveer 3 minuten worden teruggebracht. Hierdoor wordt de inzetijd met ongeveer 5 minuten verlengd (zie figuren 5.8 en 5.9).

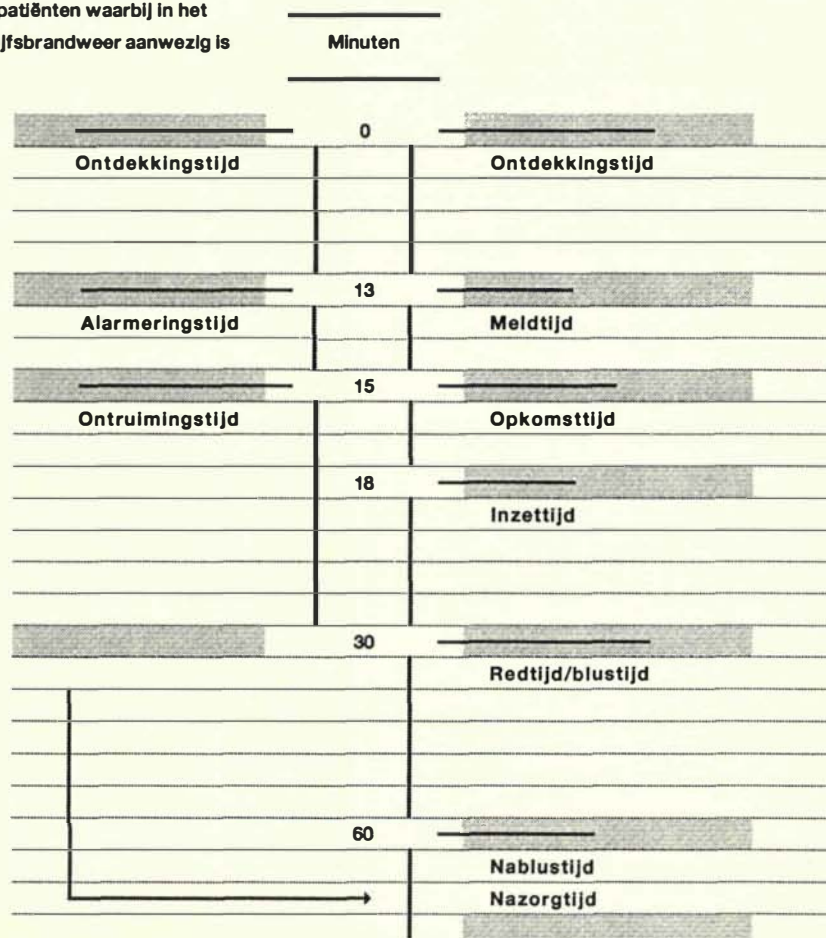
Gelet op de hiervoor beschreven fysieke mogelijkheden van het brandweerpersoneel is de maximale hoogte voor gezondheidszorggebouwen zonder brandweerlift en blusleiding (ook met langere inzetijd) vooralsnog ongeveer 20 meter.

46

Oefening in een ziekenhuis



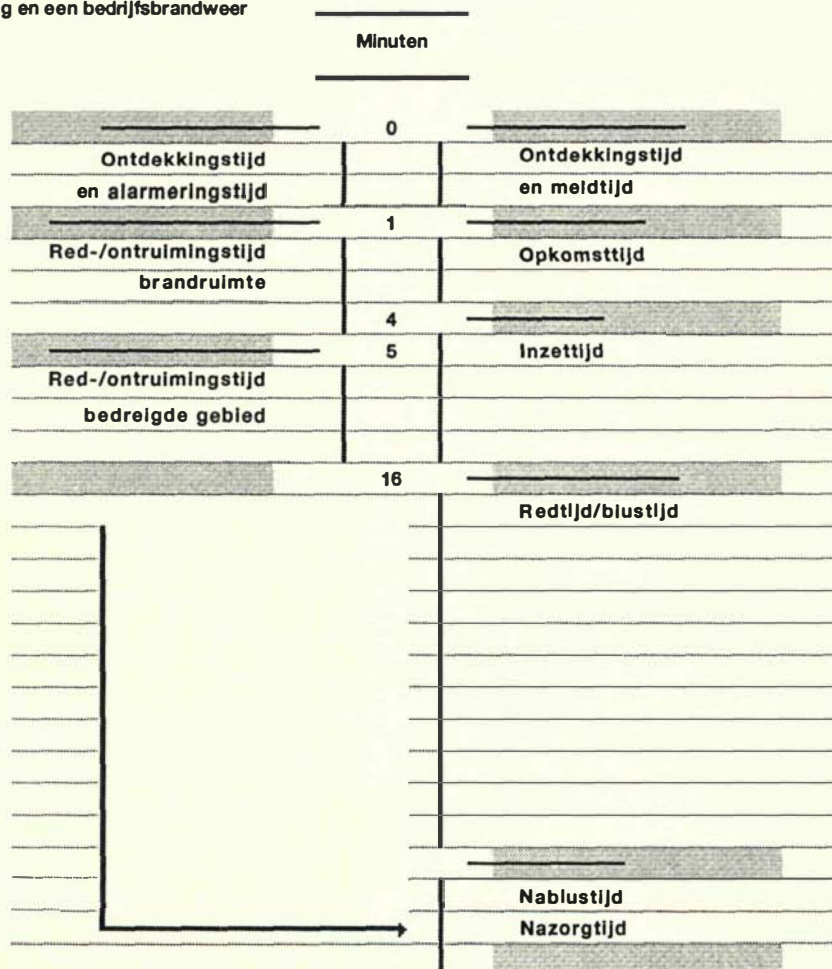
Figuur 5.8 Fasen in een normatief brandverloop in een gezondheidszorggebouw met zelfredzame patiënten waarbij in het gebouw een bedrijfsbrandweer aanwezig is



Overleg aanvalsplan

47

Figuur 5.9 Fasen in een normatief brandverloop in een gezondheidszorggebouw met niet-zelfredzame patiënten waarbij in het gebouw een brandmeldinstallatie met volledige bewaking en een bedrijfsbrandweer aanwezig zijn



4 Het voorkomen van een brandweerinzet door de brand vrijwel direct na het ontstaan automatisch te blussen of onder controle te hebben (blustijd < 5 minuten)

Door het toepassen van een automatische sprinklerinstallatie kan een brand geblust of ten minste onder controle worden gehouden. Hierdoor blijft de inzet van de brandweer beperkt tot een nacontrole (zie figuren 5.6 en 5.7).

48

Flevoziekenhuis, Almere
Campaman, Tennekes, de Jong Architecten

5.3 Plaatselijke afwijkingen in opkomsttijd en brandweersterkte

Het brandbeveiligingsconcept gezondheidszorggebouwen is onder andere bedoeld voor het op één lijn brengen van de landelijke regelgeving met betrekking tot de brandveiligheid. In het brandbeveiligingsconcept is voor de bepaling van de opkomsttijd van de brandweer en het aantal brandweereenheden gebruik gemaakt van de aanbevelingen uit de 'handleiding Brandweezorg'.

Op lokaal niveau kunnen opkomsttijd en brandweersterkte afwijken van deze waarden. Hierdoor kan het voorkomen dat voor een bepaald gezondheidszorggebouw in een gemeente het in dit brandbeveiligingsconcept omschreven brandveiligheidsniveau niet wordt gehaald.

Met de in dit brandbeveiligingsconcept beschreven systematiek kan een gemeente er zelf voor zorgdragen, dat in dat bepaalde gezondheidszorggebouw het brandveiligheidsniveau toch wordt gehaald. Hierbij kan vooral worden gedacht aan zwaardere voorzieningen, respectievelijk maatregelen ten aanzien van de brandmelding en/of de interne organisatie van het gezondheidszorggebouw.

Voor gezondheidszorggebouwen met niet zelfredzame patiënten zijn de mogelijkheden voor uitwisseling beperkt.

Één en ander laat zich schematisch weergeven in figuur 5.1, de brandveiligheidsbalans. Waarbij aangetekend dient te worden, dat deze uitwisseling niet in conflict mag zijn met gemeentelijke of rijksregelgeving.

49

5.4 Samenvatting

Vanuit een normatief brandverloop en een gebeurtenissenboom worden de brandbeveiligingsmaatregelen en -voorzieningen geformuleerd.

Deze maatregelen en voorzieningen zijn onderverdeeld in:

- planologie
- bouwkunde
- installatie-techniek
- inventaris
- interne organisatie en gebruik
- inzet brandweer.

Gezondheidszorggebouwen zouden altijd aan deze maatregelen en voorzieningen moeten voldoen. Indien niet kan worden voldaan aan de in het normatief brandverloop vermelde tijden, kan het treffen van aanvullende brandbeveiligingsmaatregelen en -voorzieningen nodig zijn.