

Verbeterde Risicoklassenindeling

Definities beveiligingsmaatregelen

De definities beveiligingsmaatregelen wordt uitgegeven onder verantwoordelijkheid van het Verbond van BeveiligingsOrganisaties (VvBO) en Het Verbond van Verzekeraars.

Dit document is een revisie van de documenten in katern 3.1. Handboek Beveiligingstechniek.

- D03/385 augustus 2003 Definities beveiligingsmaatregelen,
- D03/390 september 2003 Nadere aanwijzingen en toelichting
- D03/391 september 2003 Toelichting op maatwerkbeveiliging
- D02/171 juni 2002 Meeneembeperkende maatregelen, en document
- 002288 mei 2001 Gevelementen woningen

Ondanks alle aan de samenstelling van deze uitgave bestede zorg, kan het Verbond van BeveiligingsOrganisaties geen aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

Inhoudsopgave

1.	Inleiding	4
1.1	Definities:	4
1.2	BORG certificering	5
1.3	Partiële beveiliging	6
1.4	Volledige beveiliging met maatwerk	6
1.5	Gelijkwaardigheid	6
1.6	Afwijkend beveiligingsplan	7
1.7	Afwijkend voldoen aan de eisen	7
1.8	Beoordelen van gelijkwaardigheid	7
1.9	Programma van eisen (PvE)	8
1.10	Risicoanalyse	8
1.11	Beveiligingsplan	9
2.	Organisatorische maatregelen	10
2.2	Niveau en omvang van de Organisatorische maatregelen	10
2.2.1	Niveau O1:	10
2.2.2	Sleutelbeheer en - gebruik	10
2.2.3	Sluitronde	10
2.2.4	Merken en registreren van waardevolle zaken	10
2.2.5	Zichtbare afwezigheid voorkomen	11
2.2.6	Beveiligingsverlichting	11
2.2.7	Gebruik van compartimenten	11
2.2.8	Buren en omwonenden	11
2.2.9	Huisregels en discipline	11
2.2.10	Opklimmogelijkheden	12
2.2.11	Tuinaanleg	12
2.2.12	Toegangscontrole	12
2.2.13	Gegevensbeveiliging	12
2.2.14	Wijzigingen en omstandigheden	12
2.2.15	In - en Uitschakelregistratie bij de PAC	13
2.2.16	Up en Downloaden	13
2.2.17	Logboek	13
2.3	Niveau O2:	14
3	Bouwkundige beveiligingsmaatregelen	14
3.1	Omvang van de bouwkundige beveiligingsmaatregelen	14
3.2	Het niveau van de bouwkundige beveiligingsmaatregelen	14
3.2.1	Niveau B0	14
3.2.2	Niveau B1	14
3.2.3	Niveau B2	15
3.2.4	Niveau B3	15
3.2.5	Glasafscherming / glasvervanging	15
3.2.6	Tralies, hekwerken en strekmetaal	15
4	Elektronische maatregelen	16
4.1	Omvang van de Elektronische maatregelen	16
4.2	Ontwerp en aanleg	16
4.3	Het niveau van de Elektronische maatregelen	16
4.3.1	Ed niveau	16
4.3.2	E1 niveau	17
4.3.3	E2 niveau	18
4.3.4	E3 niveau	19
4.3.5	Eisen aan alarmapparatuur:	20
4.3.6	Brandpreventie (brand) rookmelders.	21
4.3.7	Beveiligingsverlichting	22
4.3.8	Camerasystemen	23
4.3.9	Toegangscontrole	23
4.3.10	Buitendetectie	24

5.	Compartimentering en Meeneembeperkende maatregelen (C/M)	24
5.1	Inleiding	24
5.2	Attractieve goederen	24
5.3	Normstelling	25
5.4	Conclusie	25
5.5	Pictogrammen, uitleg en voorbeelden	26
5.6	C/M 1 niveau prestatie-eis 3 minuten inbraakvertraging	26
5.6.1	Verplaatsen	26
5.6.2	Koppelen	26
5.6.3	Verankeren	27
5.7	C/M 2 niveau prestatie-eis 5 minuten inbraakvertraging	27
5.7.1	Kisten of kasten	27
5.7.2	Vitrines	28
5.7.2	Hekwerken	28
5.8	C/M 3 Niveau prestatie-eis 10 minuten inbraakvertraging	28
5.8.1	Compartimenten	28
5.8.2	Kluizen en safes	30
5.8.3	Mistgeneratoren	31
6.	Alarmering	31
6.1	Voorgeschiedenis:	31
6.2	Europese normen	32
6.3	Kenmerken	33
6.4	Aanvullende bepalingen	34
6.4.1	Alarm over IP	35
6.4.2	Back-up verbinding (EN 50136-1-1 artikel 6.3.4)	36
6.4.3	Prestatieniveau AL1, AL2	36
6.4.4	Internet	36
6.4.5	Besloten netwerk/verbinding	36
6.4.6	VPN:	36
6.4.7	Voorkeurschakeling	36
6.5	ALO traject	38
6.6	AL 1 traject	38
6.7	AL 2 traject	38
6.8	AL 3 traject	39
6.9	Tips om nodeloos alarm te voorkomen	39
6.9.1	Bij aanschaf	39
6.9.2	Nieuwe alarminstallatie in gebruik nemen	39
6.9.3	Toch nodeloos alarm?	39
6.9.4	Voorkom nodeloos alarm	39
7	Reactie (alarmopvolging)	40
7.1	Indeling in niveaus	40
7.2	R0 niveau	40
7.3	R1 niveau	40
7.4	R2 niveau	40
7.5	R3 niveau	40
7.6	Alarmverificatie	41
7.7	alarmverificatie methoden	41
8	Bijlage 1. Modelformulier Programma van Eisen (PvE)	42

1. Inleiding

In dit document worden de beveiligingsmaatregelen gedefinieerd en toegelicht die volgens de systematiek van de risicoklassen worden vereist voor de inbraakbeveiliging van een woning of bedrijf. Dit betreft de omschrijving van de O,B (M/C),E, A en R maatregelen en waaraan deze op de verschillende niveaus moeten voldoen. Allereerst wordt er echter op gewezen dat het mogelijk - en soms nodig of beter - is om 'afwijkingen' toe te passen. Want afwijkingen in de hier gehanteerde systematiek en in het voldoen aan de eisen zijn soms nodig of leiden tot betere oplossingen. In verband daarmee wordt het begrip 'gelijkwaardigheid' geïntroduceerd.

Daar waarin dit document en andere publicaties wordt gesproken over het niveau 1, 2 of 3 mag ook worden verstaan: respectievelijk niveau: 's' (standaard), 'n' (normaal) en 'z' (zwaar).

1.1 Definities:

BORG technische beveiligingsbedrijf

Een natuurlijke of rechtspersoon wat op grond van de Nationale Beoordelingsrichtlijn voor het BORG procescertificaat voor Ontwerpen, Uitvoeren, en Onderhouden van Inbraakbeveiliging is gecertificeerd voor deelgebied 1, 2 en 3.

BORG alarminstallateur

Een natuurlijke of rechtspersoon wat op grond van de Nationale Beoordelingsrichtlijn voor het BORG procescertificaat voor Ontwerpen, Uitvoeren, en Onderhouden van Inbraakbeveiliging is gecertificeerd voor deelgebied 1.

BORG bouwkundig beveiligingsbedrijf

Een natuurlijke of rechtspersoon wat op grond van de Nationale Beoordelingsrichtlijn voor het BORG procescertificaat voor Ontwerpen, Uitvoeren, en Onderhouden van Inbraakbeveiliging is gecertificeerd voor deelgebied 3.

Alarminstallatie

Samenstel van componenten waarmee een onveilige situatie kan worden gesignaleerd en via telecommunicatie doorgegeven aan één of meer centrale punt(en), waar die signalen worden ontvangen en beoordeeld en van waaruit assistentie kan worden gevraagd aan derden. (noot)

Noot: Daar waarin dit document en andere publicaties wordt gesproken over Alarminstallatie moet ook worden verstaan:

"elektronische beveiliging", inbraaksignalering(s)systeem, inbraaksignalering(s) installatie, inbraakalarmsysteem, inbraakalarminstallatie, alarmsysteem, (inbraak) alarmapparatuur e.d. Inhoudelijk wordt bedoeld:

Alarmapparatuur en componenten vormen samen een alarmsysteem voor het detecteren en signaleren van inbraak of pogingen daartoe, al dan niet tevens voor het signaleren van brand(rook) technische meldingen en/of een overval. Het gestelde in de Wet particuliere beveiligingsorganisaties en recherchebureaus is onverminderd van toepassing.

Beveiligingssysteem

Een samenhangend systeem van bouwkundige - mechanische -, compartimentering -, meeneembeperkende -, elektronische -, alarmerende - en reagerende maatregelen. Beveiligingsprocessen en procedures (organisatorische maatregelen) maken deel uit van het geheel. Een alarminstallatie is hiervan slechts een onderdeel.

PAC (particuliere alarmcentrale)

Een particuliere onderneming die in de uitoefening van beroep of bedrijf ten behoeve van derden in een centraal alarmmeldpunt, de door alarmapparatuur verzonden signalen ontvangt en beoordeelt en zonodig assistentie vraagt aan de politie, andere overheidsinstanties of particulieren. (noot)

Noot: Een PAC is beveiligingsorganisatie als bedoeld in de Wet particuliere beveiligingsorganisaties en recherchebureaus, artikel 3, sub b. en een 'Alarm receiving centre' artikel 4.2 in de NEN-EN 50136-1-1

1.2 BORG certificering

Voor iedere beveiligingsklasse wordt in de ‘indeling in risicoklassen’ een beveiligingsconcept gegeven in de vorm van een combinatie van de O, B, E en R maatregelen. Indien het beveiligingsconcept volgens een bepaalde klasse wordt gerealiseerd is het BORG technische beveiligingsbedrijf volgens de BRL BORG 2005 versie 2 verplicht tot de afgifte van een ‘BORG Beveiligingscertificaat’. Het certificaat zegt daarom niet alleen iets over de kwaliteit van de toegepaste componenten en de manier waarop ze zijn verwerkt, maar vooral ook over de samenhang en het beveiligend vermogen ervan.

Heel concreet betekent het voorgaande dat het BORG Beveiligingscertificaat aangeeft dat alle conform de bepaalde beveiligingsklasse vereiste beveiligingsmaatregelen zijn uitgevoerd (volgens de desbetreffende voorschriften) of daaraan gelijkwaardig is (maatwerk).

Indien de beveiliging bestaat uit alleen de bouwkundige maatregelen wordt een BORG Opleveringsbewijs bouwkundige beveiliging afgegeven. Wel dient het opleveringsbewijs het niveau van de maatregel te worden omschreven dus: B1, B2 of B3 of B1+C/M 1, respectievelijk B1+C/M 2 of B1+C/M 3. De geleverde maatregelen worden daarmee **object gebonden in plaats van risico gebonden**.

Bij een gedeeltelijke uitvoering van de beveiligingsmaatregelen, dat wil zeggen uitsluitend de E (+O, A en R) maatregelen, wordt een BORG Opleveringsbewijs alarminstallatie afgegeven.

Hiervoor geldt dat de beveiligingsmaatregelen moet voldoen aan het niveau van de geconstateerde beveiligingsklasse. Het vereiste niveau van de “Elektronische maatregelen” wordt bepaald door de risicoklasse (voor wat betreft de eisen aan het alarmtransmissiesysteem) en de beveiligingsklasse (voor wat betreft O, E en R maatregelen).

Als basis daarvoor is de risicoklasse bepaald op basis van categorie attractieve goederen in eigen gebruik, in winkel of in opslag/magazijn (zie tabel in bijlage 1 document D03/376 versie mei 2007) en voor welke waarde die goederen aanwezig zijn. Daarbij is het niveau van de E maatregel in de beveiligingsklasse 3 en 4 ook gekoppeld aan de uitvoering van de Bouwkundige en C/M maatregelen (zie kolom ‘voorwaarden’ in tabel 2 in document D03/376 versie mei 2007).

Indien niet wordt gekozen C/M maatregelen is voor de E maatregel een extra eis van toepassing namelijk: schildetectie (geveldetectie) op niveau 2 respectievelijk niveau 3.

Belangrijk is dus dat u zich realiseert dat wanneer u alleen de E maatregelen uitvoert (in klasse 3 of 4) moet uitgaan van de aanvullende eis voor schildetectie (geveldetectie) om te voldoen aan de doelstelling dat uw deeloplossing (BORG Opleveringsbewijs alarminstallatie) wel conform de geconstateerde risicoklasse is.

Indien u beveiligingsplan daarin niet voorziet (of wanneer u daar geen opdracht voor krijgt) en in gevallen waar de verzekeraar geen eisen stelt mag u ook op een lager niveau een BORG Opleveringsbewijs alarminstallatie afgeven. De geleverde maatregelen worden daarmee **alarminstallatie gebonden in plaats van risico gebonden**.

Er kan echter ook worden besloten om een afwijkend beveiligingsplan op te stellen; dit is maatwerk. Na het volgen van de hiervoor omschreven procedure wordt het BORG Beveiligingscertificaat afgegeven. De inschalingmethode die in de ‘indeling in risicoklassen’ wordt gehanteerd, is in feite niet bedoeld voor (zeer) grote of bijzondere objecten, want het optimale beveiligingsconcept kan hiervoor niet gemakkelijk gevangen worden in een standaard aanpak. Het opstellen van een beveiligingsconcept voor dit soort objecten is daarom meestal maatwerk. Bij het beveiligen van grote of bijzondere objecten kunnen zich twee situaties voordoen:

1. de attractieve zaken bevinden zich slechts in een beperkt deel van het object (bijvoorbeeld in het kantoor van een betonwarenfabriek) of een deel van het object valt in een hogere klasse (bijvoorbeeld magazijn/opslag);
2. het gehele object dient op een maatwerkmanier te worden beveiligd.

1.3 Partiële beveiliging

In het hiervoor genoemde eerste geval kan het voldoende zijn om alleen het meest risicovolle deel van het object te beveiligen. Er is dan in feite sprake van partiële beveiliging van het object, waarbij voor het bepalen van de beveiligingsaanpak in principe gebruik gemaakt kan worden van de systematiek volgens het deel 'indeling in risicoklassen'. Indien deze werkwijze wordt gevolgd, kan vervolgens een 'gewoon' BORG Beveiligingscertificaat worden afgegeven voor het beveiligde gebouw(gedeelte). Daarbij dient duidelijk te worden vastgelegd op welk gebouw(gedeelte) het certificaat betrekking heeft. Voorwaarde is hierbij wel dat het gaat om een apart gebouw op het desbetreffende complex of om een afgescheiden gebouwgedeelte.

Bij een afgescheiden gebouwgedeelte dient de scheidingsconstructie (de scheidingswanden e.d.) met de rest van het gebouwencomplex te voldoen aan dezelfde bouwkundige (inbraakwerendheid)eisen als die voor de buitengevels (daken etc.) van het beveiligde gedeelte. Inbraaktechnisch gezien dient het beveiligde gebouwgedeelte dus als zelfstandig gebouw te worden behandeld.

Indien de hiervoor bedoelde scheidingsconstructie ontbreekt of onvoldoende inbraakwerendheid bezit, kan de hier geschetste werkwijze niet worden gevolgd. Er dient dan een compleet beveiligingsplan (maatwerk) voor het geheel te worden gemaakt.

Een tweede mogelijkheid kan zich voordoen dat een gedeelte van het object waar zich concentraties van attractieve goederen bevinden (magazijn/opslag) die door de inschaling in een hogere risicoklasse valt dan het overige deel van het object (kantoren en/of productieruimten) in dat geval kan er voor de verschillende bouwdelen een op het risico afgestemd pakket van maatregelen worden vastgesteld. In dit voorbeeld is de procedure voor volledige beveiliging met maatwerk noodzakelijk.

1.4 Volledige beveiliging met maatwerk

Bij het opstellen van een maatwerk beveiligingsplan dient onderstaande procedure te worden gevolgd. Zoals hiervoor aangegeven kan dit betrekking hebben op objecten in alle risicoklassen

Het gaat er hierbij immers om dat geen standaardoplossing volgens de 'indeling in risicoklassen' wordt toegepast, maar dat een beveiligingsplan als maatwerk wordt opgesteld. Na uitvoering en na het volgen van de juiste procedure kan een BORG Beveiligingscertificaat worden afgegeven.

Bij de procedure voor maatwerk is het van belang dat er van tevoren overeenstemming bestaat over het beveiligingsplan. Hiertoe dienen de uitgangspunten te worden vastgelegd in het programma van eisen. Om te vermijden dat er verschillen van inzicht ontstaan, dienen alle betrokken partijen bij risicoklasse 4 schriftelijk te verklaren in te stemmen met (de uitgangspunten van) het beveiligingsplan. Vooral instemming van de desbetreffende verzekeraar is van belang. Desgewenst kan advies worden ingewonnen bij een inspectie-instelling. Indien één van de betrokken partijen dit wenst of eist kan worden afgesproken dat bij oplevering een opleveringsinspectie plaatsvindt door een inspectie-instelling op basis van ISO/IEC 17020-A en bevoegd voor inbraakbeveiliging conform de BRL BORG 2005 versie 2

1.5 Gelijkwaardigheid

Ten aanzien van het begrip 'gelijkwaardigheid' doen zich twee situaties voor:

- het beveiligingsplan dat op een afwijkende, maar gelijkwaardige manier wordt ingevuld;
- de beveiligingsmaatregelen waaraan op een afwijkende, maar gelijkwaardige manier, wordt voldaan.

Beide 'afwijkingen' worden hierna nader toegelicht.

1.6 Afwijkend beveiligingsplan

In de risicoklassenindeling worden de vereiste beveiligingsmaatregelen in de beveiligingsklassen 1, 2, 3 en 4 aangegeven met de letters O, B, E en R, waarbij het benodigde niveaus wordt weergegeven door de cijfers 0, 1, 2 en 3. In de meest voorkomende gevallen wordt zo door een combinatie van letters en cijfers een adequaat pakket beveiligingsmaatregelen weergegeven voor het desbetreffende object of deel daarvan. Men dient er echter op bedacht te zijn dat er hierdoor sprake is van een zekere standaardisering die niet altijd tot een optimaal resultaat behoeft te leiden.

Voor zulke gevallen is het beter om een (iets) afwijkend pakket maatregelen samen te stellen. En dat is - in de hier gehanteerde systematiek - mogelijk door gebruik te maken van het beginsel 'gelijkwaardigheid'. Dat wil zeggen door het toepassen van maatregelen die samen leiden tot een resultaat dat 'gelijkwaardig' is aan dat van de maatregelen die in de desbetreffende beveiligingsklasse zijn voorgeschreven.

Het voorgaande is zeker van toepassing in de gevallen dat sprake is van een hoog inbraakrisico. Daarom is vermeld dat de vereiste beveiligingsmaatregelen ook volgens 'maatwerk' kunnen worden uitgevoerd. Dat wil zeggen dat een pakket maatregelen moet worden gekozen dat precies is toegesneden op het desbetreffende object. Hoe dat pakket eruit moet zien is niet gemakkelijk vast te leggen in een standaardoplossing.

Ook in dit opzicht echter is er sprake van 'gelijkwaardigheid', want het beveiligend vermogen van de maatwerkoplossing moet gelijkwaardig zijn aan hetgeen ten minste vereist is in de van toepassing zijnde beveiligingsklasse. De juiste invulling voor het desbetreffende object is echter een kwestie van maatwerk.

1.7 Afwijkend voldoen aan de eisen

De omschrijving van de beveiligingsmaatregelen in de risicoklassenindeling: definities beveiligingsmaatregelen gebeurt zoveel mogelijk in de vorm van prestatie-eisen. Dat wil zeggen dat niet precies wordt aangegeven op welke manier aan de eisen moet worden voldaan, maar wél welke prestatie geleverd moet worden. Dit geeft de mogelijkheid om voor een bepaald object de meest geschikte oplossingen te kiezen uit de (vele) verschillende mogelijkheden tot beveiliging. Bij het formuleren van prestatie-eisen wordt verwezen naar normen en voorschriften. Op basis daarvan kan worden geverifieerd of een bepaalde oplossing de gevraagde prestatie levert. Zulke normen en voorschriften bestaan echter niet op alle gebieden van inbraakpreventie en daarom wordt in een aantal gevallen omschreven hoe de gevraagde beveiligingsmaatregel eruit moet zien. Het is daarbij uitdrukkelijk niet de bedoeling om alternatieve oplossingen uit te sluiten. Vooral niet als die tot een beter resultaat leiden! Bij het toepassen van alternatieve oplossingen dient daarom eveneens het begrip 'gelijkwaardigheid' te worden gehanteerd: de gekozen oplossing dient ten minste gelijkwaardig te zijn aan de voorgeschreven maatregel.

1.8 Beoordelen van gelijkwaardigheid

Door wie (of hoe) wordt de gelijkwaardigheid nu beoordeeld? Bij producten, constructies of installaties waarvoor genormaliseerde beproevingen of voorschriften bestaan, ligt dat tamelijk eenvoudig. De beoordeling kan hier plaatsvinden aan de hand van testresultaten of de desbetreffende voorschriften. In andere gevallen is dat niet mogelijk en zal de beoordeling moeten plaatsvinden op grond van vakkennis en ervaring. Het beoordelingsvermogen van de deskundige moet hierbij niet worden onderschat, maar dit sluit de mogelijkheid niet uit dat andere deskundigen tot andere conclusies komen. Bij de toepassing van het beginsel van gelijkwaardigheid is het daarom altijd van belang dat de direct betrokkenen vooraf tot overeenstemming komen. Dit moet middels het vastleggen van de maatwerkoplossingen in het PvE (programma van eisen) waarin de eisende partijen zich akkoord verklaren.

1.9 Programma van eisen (PvE)

In de BRL BORG 2005 versie 2 is vermeld (artikel 4.2.3):

De certificaathouder legt, in overleg met de opdrachtgever, het programma van eisen voor het beveiligingsplan vast in een document, genaamd Programma van Eisen (PvE).

De eisen waaraan het PvE moet voldoen zijn niet nader omschreven in de BRL BORG 2005 versie 2.

Als basis voor dit document gaan we op hoofdlijnen uit van een document conform: CLC/TS 50137-7: 2003 annex F. Het PvE bevat:

NAW gegevens van de klant (opdrachtgever) en de aanduiding van het object,

De geconstateerde risicoklasse, de gekozen combinatie van de daarbij behorende beveiligingsklasse in de vorm van een aanduiding van de individuele niveaus uitgesplitst in:

O: Organisatorische maatregelen

B: Bouwkundige maatregelen + indien van toepassing, de C/M maatregelen

E: Elektronische maatregelen + Alarmering

R: Reactie (alarmopvolging)

Bij afwijkingen wordt onder “maatwerk” een toelichting gegeven.

Een verwijzing naar het beveiligingsplan (voor zover dit in dit stadium reeds beschikbaar is)

De vermelding van het kwaliteitsdocument wat na oplevering wordt afgegeven.

Autorisatie van het ingevulde document.

De functie van het PvE is vergelijkbaar met het bronformulier uit een voorgaande regeling.

Voorbeeld sjabloon PvE: zie bijlage 1

1.10 Risicoanalyse

De risicoanalyse gaat minimaal uit van onderstaande gegevens:

Woningen

Attractieve zaken van de inboedel:

Audiovisuele en computerapparatuur: vastgestelde waarde €.....

Lijfsieraden en contact geld of waardepapieren: vastgestelde waarde €.....

Bijzondere bezittingen: vastgestelde waarde €.....

Immateriële zaken die van toepassing zijn op het risico waardoor de uitkomst in een hogere risicoklasse wordt ingeschaald dan de optelling van de attractieve zaken van de inboedel rechtvaardigen, alsmede specifieke risico's en maatregelen die in het beveiligingsplan zijn/worden uitgewerkt.

Bedrijven

Attractieve goederen categorie L: vastgestelde waarde €.....

Attractieve goederen categorie M: vastgestelde waarde €.....

Attractieve goederen categorie H: vastgestelde waarde €.....

Attractieve goederen categorie ZH: vastgestelde waarde €.....

Immateriële zaken die van toepassing zijn op het risico waardoor de uitkomst in een hogere risicoklasse wordt ingeschaald dan de uitkomst m.b.t. de attractieve goederen en bedrijfsuitrusting / inventaris rechtvaardigen, alsmede specifieke risico's en maatregelen die in het beveiligingsplan zijn of worden uitgewerkt.

1.11 Beveiligingsplan

Het beveiligingsplan bevat:

- een aanduiding van het te beveiligen (deel van het) bouwwerk of terrein,
- een aanduiding van de doelstelling van de beveiliging, waarbij de materiële - en immateriële - attractieve zaken worden genoemd, waarop de beveiliging is toegespitst, de risicoanalyse en de uitkomst van de risicoanalyse (zie 4.2.2 en 4.3.1 van de BRL BORG 2005 versie 2) met vermelding van de geconstateerde risicoklasse, en een aanduiding van de te treffen maatregelen volgens de, bij de risicoklasse behorende, beveiligingsklasse.

Vastgelegd moet worden of de beveiliging moet geschieden op basis van een beveiligingssysteem (afgifte van een BORG Beveiligingscertificaat), of op basis van een BORG Opleveringsbewijs.

Is het uitgangspunt een beveiligingssysteem dan bevat het beveiligingsplan voor alle maatregelen een specificatie van de te treffen O, B (+ indien van toepassing C/M), E (+ AL) en R maatregelen. Inclusief de projecteringstekening(en). Bij kleine objecten kan ook worden volstaan met een aanduiding in plaats van een projecteringstekening.

Is het uitgangspunt een BORG Opleveringsbewijs alarminstallatie voor de elektronische maatregelen dan bevat het beveiligingsplan een specificatie van de E (+AL) en R alsmede de daarbij behorende organisatorische maatregelen. Inclusief de projecteringstekening(en) van de alarminstallatie. Bij kleine objecten kan ook worden volstaan met een aanduiding in plaats van een projecteringstekening.

Is het uitgangspunt een BORG Opleveringsbewijs bouwkundige beveiliging dan bevat het beveiligingsplan een specificatie van B, en eventuele C/M maatregelen alsmede de daarbij behorende organisatorische maatregelen.

Leeswijzer:

Aanduiding: benaderende beschrijving

Specificatie: iedere maatregel op zich zelf noemen

2. Organisatorische maatregelen

Indeling in niveaus

Afhankelijk van de van toepassing zijnde beveiligingsklasse zijn niveaus in de organisatorische maatregelen voorgeschreven. We onderscheiden twee verschillende niveaus, O1, en O2. Een deel van de eisen die voorheen werden vermeld bij de Elektronische maatregelen maar hoofdzakelijk van organisatorische aard zijn, zoals bijvoorbeeld het bewaken van in - en uitschakeltijden van de alarminstallatie, zijn nu bij de O maatregelen opgenomen.

2.2 Niveau en omvang van de Organisatorische maatregelen

2.2.1 Niveau O1:

Standaard organisatorische maatregelen en voorlichting over preventie. Inbraakpreventie is niet alleen een kwestie van het treffen van bouwkundige en elektronische maatregelen. Om tot een sluitend geheel te komen zal de eigenaar of gebruiker van een beveiligde woning of gebouw moeten zorgen dat ook de nodige organisatorische maatregelen worden getroffen. Hierbij ligt het voor de hand dat de technische preventieve voorzieningen op de juiste manier gebruikt moeten worden, om deze het gewenste effect te laten sorteren. Daarnaast zal - om te zorgen dat dit ook in de toekomst het geval zal zijn - het onderhoud daarvan geregeld moet worden. En ten slotte zijn er tal van organisatorische maatregelen die het de inbreker moeilijk maken of die hem soms al van tevoren doen besluiten af te zien om van een poging tot inbraak of diefstal.

Het totale pakket organisatorische maatregelen zal van geval tot geval verschillen; het is sterk afhankelijk van de situatie. Er zijn voldoende publicaties voorhanden die aandacht besteden aan de volgende standaard onderwerpen. Deze behoren bij oplevering van een alarminstallatie of het beveiligingssysteem aan de gebruiker te worden overhandigd.

2.2.2 Sleutelbeheer en - gebruik

Een slot moet goed gebruikt worden, anders heeft het geen zin. In elk geval moet ervoor worden gezorgd dat alleen bevoegde personen in het bezit zijn van een sleutel en dat eventuele reservesleutels goed worden opgeborgen. Om het aantal in gebruik zijnde sleutels te beperken, kan gebruik gemaakt worden van gelijksluitende cilinders. De inbraakwerende eigenschappen van sloten zijn gebaseerd op een situatie dat het slot op het nachtslot zit en de sleutel uit het slot is gehaald, dit voorkomt ook dat door middel van flipperen (terugduwen van de dagschoot met behulp van bijvoorbeeld een betaalpasje) de deur kan worden geopend. Zelfs als de bewoners thuis zijn en bijvoorbeeld slapen. Bij bedrijven verdient het aanbeveling om te registreren wie een sleutel in gebruik heeft. Er dient, met name bij bedrijven, een meldingsplicht te zijn bij verlies van een sleutel.

2.2.3 Sluitronde

Bij het afsluiten van het gebouw - en eventueel het inschakelen van de alarminstallatie - dient te worden gecontroleerd of alle ramen en deuren zijn afgesloten. Maak daar een vaste afsluitronde van; dit beperkt de kans om een deur of raam te vergeten. Maak duidelijke afspraken over wie er verantwoordelijk is voor het afsluiten en wie er als plaatsvervanger optreedt. Bij zeer hoge risico's en bij objecten waar een bepaalde cultuur heerst dat niemand zich verantwoordelijk voelt (vergelijkbaar met scholen) kan mogelijk (O2) een gedwongen sluitronde worden ingevoerd: alle ruimtelijk werkende detectoren moeten zijn "uitgelopen" anders kun je niet inschakelen.

2.2.4 Merken en registreren van waardevolle zaken

Voorzie de meest waardevolle zaken van postcode en huisnummer door middel van graveren, etsen of inbranden. Registreer deze bezittingen op een lijst en maak er eventueel foto's van. Na een diefstal kan dit nuttig zijn voor herkenning en opsporing en voor het vaststellen van de schade.

2.2.5 Zichtbare afwezigheid voorkomen

Vooraf in vakantieperiodes is een bekend verschijnsel dat gesloten gordijnen, overvolle brievenbussen, niet gemaaid gazons en zelfs briefjes op de deur afwezigheid kunnen verraden. Deze signalen maken de keuze voor de inbreker er niet moeilijker op. Buren, kennissen of familieleden kunnen helpen om een huis bewoond te laten lijken. Het laten branden van enkele lichtpunten in het huis accentueert het bewoond uiterlijk. Door middel van instelbare schakelklokken kan met enkele lichtpunten - met energiezuinige lampen - in het huis een normaal bewoningspatroon worden gesimuleerd. Bij bedrijfspanden is nachtverlichting preventief en een maakt het tevens mogelijk voor alarmopvolgers zich te oriënteren.

2.2.6 Beveiligingsverlichting

Een inbreker wordt niet graag gezien. Vandaar dat beveiligingsverlichting langs de buitenkant van het gebouw preventief werkt indien de omgeving (sociale) controle toelaat en de inbreker inderdaad de kans loopt om gezien te worden. Beveiligingsverlichting kan door middel van een schemerschakelaar automatisch worden ontstoken en gedoofd. Het verlichtingsniveau dient - met name ter plaatse van deuren, ramen en opklimmogelijkheden - ten minste gelijk te zijn aan dat van de openbare verlichting. In bepaalde gevallen kan 'schrikverlichting' worden toegepast, die wordt ingeschakeld door een detector of door de alarminstallatie.

2.2.7 Gebruik van compartimenten

Indien in het gebouw een inbraakwerend compartiment is ingericht, dienen afspraken te worden gemaakt over het gebruik van deze ruimte. Maak duidelijke afspraken over wie er verantwoordelijk is voor het goede gebruik van het compartiment en wie als plaatsvervanger optreedt. Het voorgaande geldt eveneens voor de (veilige) opslag van vertrouwelijke documenten, databestanden e.d.

2.2.8 Buren en omwonenden

Het verdient aanbeveling om met buren of omwonenden afspraken te maken over het in de gaten houden van elkaars gebouwen. In woonwijken kan dit worden georganiseerd in de vorm van buurtpreventie projecten. Bewoners kunnen zo, samen met de politie, zorgen dat inbrekers en vandalen minder makkelijk de kans krijgen hun slag te slaan. Op bedrijventerreinen en in winkelcentra wordt de bewaking in toenemende mate georganiseerd in samenwerking met particuliere beveiligingsbedrijven, gemeente en politie.

2.2.9 Huisregels en discipline

Hoe compleet de technische beveiliging ook is opgezet, alle techniek wordt tenietgedaan door gebrek aan discipline of het ontbreken van sluitende huisregels. Met name voor bedrijven is het van belang dat huisregels worden opgesteld die antwoord geven op de volgende vragen.

- Wie mag waar komen?
- Wie mag wanneer ergens komen?

Welke andere beperkingen van de bewegingsvrijheid zijn nodig en voor welke mensen: personeelsleden, inleenkrachten, leveranciers, bezoekers etc.

- Welke gegevens zijn voor wie toegankelijk?
- Waar en hoe worden ze opgeborgen?
- Welke gegevens en andere zaken zijn moeilijk vervangbaar en dienen daarom diefstal - (en brand) werend te worden opgeborgen?

2.2.10 Opklimmogelijkheden

Opklimmogelijkheden om het gebouw dienen zoveel mogelijk vermeden te worden. Inbrekers schrikken er niet voor terug om via opklimmogelijkheden, zoals afvalcontainers, afdaken, een stapel pallets, een ladder, de afdekkap van de zonwering e.d., naar boven te klimmen om te onderzoeken of ze niet makkelijker binnen kunnen komen via daklichten, dakramen, bovenlichten of balkondeuren. Opklimmen kan worden bemoeilijkt door het toepassen van bijvoorbeeld getande beugels rond hemelwaterafvoeren en overklimbeveiliging op (lage) muren. Losse hulpmiddelen, zoals ladders, pallets, kratten, verrolbare containers e.d., dienen te worden opgeborgen of met een goed hangslot op hun - van het gebouw verwijderde - plaats te worden gefixeerd. Speciale aandacht verdienen in dit verband ook tijdelijke voorzieningen, zoals bijvoorbeeld de steiger van een schilder. Bij bedrijven is extra aandacht voor opklimmogelijkheden een must. Veel daders plegen inbraken via de daken. Na een veroorzaakt alarm kijkt een alarmopvolger vaak alleen na verbreking van de schil; het dak wordt zelden gecontroleerd. Inbrekers weten dit en maken hiervan handig gebruik.

2.2.11 Tuinaanleg

Bij de aanleg en het onderhoud van de beplanting rondom het gebouw dient ervoor te worden gezorgd dat het geheel overzichtelijk blijft. Het is van belang dat de inbreker niet ongezien te werk kan gaan door hoogopgaande begroeiing of zich hierin kan verschuilen. Het verdient aanbeveling om de hoogte van de begroeiing om het gebouw te beperken tot circa 1 meter. Het is goed om hiermee rekening te houden bij de keuze van de beplanting en ook om bij het tuinonderhoud het onderwerp inbraakpreventie niet uit het oog te verliezen. Toepassing van doornachtige beplanting kan de toegankelijkheid verminderen. Het toepassen van een hekwerk om het terrein maakt het betreden natuurlijk nooit geheel onmogelijk, maar een hek vormt wel een extra barrière. Ook voor vandalen en ook bij de eventuele afvoer van de buit. Bovendien vormt het hek een juridische afscherming. Iemand die je aantreft achter een hek is in overtreding, artikel 461 Sr.

2.2.12 Toegangscontrole

Voor bedrijven verdient het aanbeveling om een vorm van toegangscontrole te organiseren om zoveel mogelijk te voorkomen dat onbevoegden het terrein of de gebouwen betreden. Enerzijds bestaan hiervoor technische hulpmiddelen, zoals speciale pasjes, anderzijds is het ook weer een kwestie van organisatie. Niet alleen via een portier of een receptioniste, maar ook via (de andere) personeelsleden die de instructie hebben om onbekenden aan te spreken en - zo nodig - te verzoeken het bedrijf te verlaten.

2.2.13 Gegevensbeveiliging

Belangrijke bedrijfsgegevens, zoals vertrouwelijke documenten, computerbestanden, tekeningen van op maat gemaakte machines, receptuur e.d., dienen zeker ook te worden gerekend tot de attractieve zaken die dienen te worden beveiligd tegen brand en diefstal. En niet te vergeten: vandalisme! Hiervoor geldt in principe alles wat is gesteld voor de beveiliging van andere attractieve zaken. En zelfs in versterkte mate indien de vermissing van belangrijke bedrijfsgegevens de bedrijfscontinuïteit in gevaar kan brengen.

2.2.14 Wijzigingen en omstandigheden

Inbraakbeveiliging is in feite altijd maatwerk, want alle beveiligingsmaatregelen worden speciaal afgestemd op de gegeven situatie. Het verdient aanbeveling om dit steeds goed in het oog te houden, zodra er plannen worden gemaakt om iets te wijzigen. Bij plannen voor verbouwing, uitbreiding, het wijzigen van de indeling, de routing of de bestemming van ruimten, dient daarom steeds te worden nagegaan of het nodig is de beveiliging aan te passen.

Dat is beter dan af te wachten tot het beveiligingsbedrijf de noodzaak tot aanpassing constateert tijdens de uitvoering van het periodieke onderhoud. Hetzelfde geldt natuurlijk ook voor wijziging met betrekking tot attractiviteit. Het beveiligingsniveau moet daarop blijvend zijn afgestemd. En wat daarbij zeker niet uit het oog mag worden verloren is de acceptatie van de gebruiker van de beveiligingsmaatregelen. ($E = K \times A$)

2.2.15 In - en Uitschakelregistratie bij de PAC

Bij gebruik van een inbraaksignaleringsysteem met aansluiting op een PAC dienen de in - en uitschakelingen te worden doorgemeld of van een (software) systeem te zijn voorzien waarbij de in -en uitschakelingen (status en tijdstip) bij een inbraakalarm worden meegezonden. Hiermee wordt bereikt dat de centralist bij een inbraakalarmmelding zicht heeft op status van de installatie. Bedieningsfouten waarbij een inbraakmelding wordt veroorzaakt zijn hierdoor herkenbaar. Een inbraakmelding die volgt binnen enkele minuten na de inschakeling zal niet worden doorgemeld naar de politie. Hetzelfde is van toepassing als er na een inbraakmelding een uitschakeling volgt naar de PAC. De centralist zal contact met het object zoeken en altijd alarmverificatie moeten toepassen alvorens de politie mag worden gewaarschuwd. Alarmverificatie is mogelijk met technische voorzieningen zoals camerabeelden, inluisteren/spreken of meerdere zones in alarm. Deze laatste optie lijdt tot negatieve alarmverificatie als er ook een in - of uitschakelmelding met een inbraakalarmmelding is binnengekomen. Als het alarm alsnog niet wordt afgemeld door de veroorzaker zal persoonlijke alarmverificatie worden aangestuurd. Dit kan overlast betekenen voor de sleutelhouder(s) of tot kosten van een particuliere bewakingsdienst.

2.2.16 Up en Downloaden

Onder uploading wordt verstaan de procedure waarbij informatie uit de alarminstallatie (met inbegrip van de daarop aangesloten randapparatuur en alarm/datatransmissieapparatuur) wordt verzonden naar een beheercomputer. De informatie behelst instellingen van parameters of software zoals die in het systeem aanwezig zijn.

Bijvoorbeeld:

- het in - of uitgeschakeld staan van het systeem en
- in - en uitloopvertragingen en het servicegeheugen.

Via een uploading procedure kunnen uitsluitend gegevens, komende uit het systeem, worden uitgelezen. Het is met deze procedure niet mogelijk parameters te wijzigen of te verwijderen. Downloading omvat de procedure waarbij via de beheercomputer commando's kunnen worden gegeven aan de centrale controle- en stuur eenheid (CCS), om de parameters of software te wijzigen. Een downloading communicatieverbinding mag slechts tot stand komen na een bewuste handeling, die moet plaatsvinden in het beveiligde object.

De bewuste handeling dient door het systeem automatisch te worden gemeld en geregistreerd bij de Particuliere Alarmcentrale (PAC) De bewuste handeling kan bestaan uit reguliere download activiteiten, waarvoor vooraf toestemming is verleend door middel van een autorisatieformulier. Na oplevering van een inbraaksignaleringsysteem dient een door de klant ondertekend autorisatieformulier met betrekking tot up- en downloading (indien van toepassing) in het dossier van de klant bij het beveiligingsbedrijf aanwezig te zijn.

2.2.17 Logboek

Bij oplevering van de alarminstallatie wordt aan de gebruiker een logboek overhandigd.

Het logboek bevat:

- Een instructie voor de gebruiker welk preventief onderhoud door gebruiker zelf periodiek dient uit te voeren.
- Een notitieblad waarop de gebruiker gebeurtenissen omschrijft, met name de ongewenste alarmeringen met vermelding van datum en mogelijke oorzaak.
- Een notieblad waarop de onderhouder (het erkende BORG bedrijf) de handelingen omschrijft bij bezoeken m.b.t. onderhoud en storingopheffing met vermelding van datum en naam van de monteur die deze werkzaamheden heeft uitgevoerd.

Bij periodieke audits (inspecties op geleverd werk) door een CI is controle hierop een onderdeel.

2.3 Niveau O2:

Als O1 met aanvulling: omschrijving van **de specifieke** organisatorische maatregelen die zijn toegespitst op het risico. Voor bedrijven geldt bovendien: bij de PAC dient registratie plaats te vinden van de in- en uitschakeltijden van het systeem, alsmede van de controlemeldingen (AL1). Schriftelijk dient te worden overeengekomen dat een overschrijding van vooraf vastgestelde tijden door de PAC dient te worden onderkend en afgehandeld conform de hierover gemaakte afspraken.

3 Bouwkundige beveiligingsmaatregelen

In de tabellen van de beveiligingsklassen voor woningen en bedrijven worden de vereiste bouwkundige maatregelen aangeduid met de letter B en een cijfer achter de B. Dit cijfer heeft betrekking op de aard en omvang (het niveau) van deze maatregelen.

3.1 Omvang van de bouwkundige beveiligingsmaatregelen

De complete bouwkundige beveiliging van een gebouw tegen inbraak moet alle inbraakgevoelige onderdelen aan de buitenzijde van een gebouw omvatten die voor inbrekers bereikbaar zijn. Dit zijn dus alle buitendeuren, ramen, lichtkoepels, dakramen e.d. Zie voor de bereikbaarheid van gevelelementen de NEN 5087. Indien een gebouw toegankelijk is via een ruimte (zoals een garage, kruipruimte of berging) waarvan de toegangsmogelijkheden vanaf het openbare gebied niet voldoen of niet kunnen voldoen aan de eisen volgens B1 respectievelijk B2 of B3, dient de scheidingsconstructie tussen deze ruimte en de rest van het gebouw te voldoen aan de eisen volgens B1 respectievelijk B2 of B3

3.2 Het niveau van de bouwkundige beveiligingsmaatregelen

Hierna volgen de omschrijvingen van de eisen waaraan de buitenschil van een gebouw (de gevels, daken e.d.) moeten voldoen.

3.2.1 Niveau B0

Het aanwezige hang- en sluitwerk waarvan niet kan worden aangetoond dat deze producten of combinaties van producten voldoen aan de BRL 3104 of niet voldoen aan weerstandsklasse 2 van de NEN 5096. "Kortom, het bestaande hang- en sluitwerk handhaven"

In voorkomende gevallen (zie tabel beveiligingsklasse in document D03-376 Risicoklassenindeling bedrijven en document D03-375 Risicoklassenindeling woningen) zijn hiervoor aanvullende E en/of C/M maatregelen vereist. Het niveau B1 heeft de voorkeur, B0 is een uitwijk mogelijkheid.

3.2.2 Niveau B1

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 2 van de NEN 5096:1998/A1:2002 nl waarmee een inbraakvertraging wordt beoogd van 3 minuten.

Voor bestaande bouw is de NEN 5089:2005 3e Ontw.nl. Inbraakwerend hang- en sluitwerk en de aanvullende eisen volgens: "BRL 3104 (1997)" van toepassing. Hierbij kan gebruik worden gemaakt van de productenlijst "genormeerde samenstelling van componenten voor gevelelementen en andere producten" bestaande bouw, meest recente uitgave, van het Centrum voor Criminaliteitspreventie & Veiligheid (CCV) Een lijst van goedgekeurde producten en productcombinaties voor deuren en beweegbare ramen en ventilatieopeningen die volgens recente beproevingen aan deze eisen voldoen is ook te vinden op de website van de SKG (www.sterrenwijzer.nl)

Ventilatie ramen of -openingen (die in het gebruik vaak open staan) met een dagmaat van minder dan 15 cm behoeven niet te worden beveiligd. Bij een grotere dagmaat dient een beveiliging tegen inklimmen te worden aangebracht.

Van kelderramen beneden het maaiveld dienen de lichtschachten te zijn afgedekt met een rooster dat met speciale beugels aan de onderzijde is vastgezet. Kelderramen boven het maaiveld kunnen het beste worden afgeschermd met traliewerk of strekmetaal. Lichtkoepels dienen, indien ze niet gemaakt zijn van slagvaste kunststof, aan de onderzijde voorzien te worden van traliewerk of strekmetaal. Slagvaste lichtkoepels dienen te zijn vastgezet met beveiligde schroeven en/of moeren.

3.2.3 Niveau B2

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 3 van de NEN 5096:1998/A1:2002 nl waarmee een inbraakvertraging wordt beoogd van 5 minuten. Voor bestaande bouw kan deze eis mogelijk ook worden bereikt door toepassing van veiligheidsbeglazing voor vaste gevelelementen weerstandsklasse 4 NEN-EN 356 P4 of zwaar traliewerk. Voor beweegbare gevelelement geldt afscherming door middel van rolluiken type O1/G1 en O2/G2 genoemd in de tabel 1 (matrix gevelafscherming) van document 002757 augustus 2001 versie 2 Handboek Beveiligingstechniek.

3.2.4 Niveau B3

Alle bereikbare gevelelementen dienen te voldoen aan de eisen volgens weerstandsklasse 4 van de NEN 5096:1998/A1:2002 nl waarmee een inbraakvertraging wordt beoogd van 10 minuten. De bouwkundige beveiliging op niveau B3 is bedoeld voor de toepassing in bedrijfsmatige objecten in de risicoklasse 4. Gelet op de aard van deze objecten moet rekening worden gehouden met 'zwaardere' aanvalsmethoden dan de gebruikelijke methoden van de gelegenheidsinbreker. Voor bestaande bouw kan deze eis mogelijk ook worden bereikt door toepassing van veiligheidsbeglazing voor vaste gevelelementen weerstandsklasse 4 NEN-EN 356 P5 of extra zwaar traliewerk. Voor beweegbare gevelelement geldt afscherming door middel van rolluiken type O3/G3 en O4/G4 genoemd in de tabel 1 (matrix gevelafscherming) van document 002757 augustus 2001 Handboek Beveiligingstechniek. Voor objecten in de risicoklasse 4 en 4* dient de invulling van de eisen volgens B3 te geschieden op basis van de risicoanalyse voor het desbetreffende object. Het PvE bevat een aanduiding van de aldus bepaalde bouwkundige maatregelen. Het beveiligingsplan bevat een specificatie van alle uit te voeren bouwkundige maatregelen.

3.2.5 Glasafscherming / glasvervanging

De afscherming van beglazing in ramen en deuren kan worden uitgevoerd door het aanbrengen van voorzieningen als tralies, hekwerken of strekmetaal. Een andere vorm van 'glasafscherming' is het aanbrengen van rolluiken, waarmee in feite een gehele pui wordt afgeschermd. Voor nadere informatie over rolluiken wordt verwezen naar document 002757 Installatievoorschriften voor rolluiken, rolhekken en schaarhekken, augustus 2001 versie 2 katern 3.2.4 Handboek Beveiligingstechniek. In plaats van het toepassen van 'glasafscherming' kan de beglazing worden vervangen door inbraakwerende beglazing. Van toepassing is: document D03/394: Inbraakwerende beglazing, september 2003 versie 2.

3.2.6 Tralies, hekwerken en strekmetaal

Bij het toepassen van tralies e.d. gaat het er om dat een inbreker - na het verwijderen/breken van de beglazing - niet makkelijk door de ontstane opening kan binnendringen. Het is van belang dat de onderlinge afstand tussen de staven van traliewerk of hekwerken zodanig klein is dat binnendringen praktisch onmogelijk wordt gemaakt. Over het algemeen is dit het geval als de ontstane openingen - na het verwijderen van het glas - een dagmaat hebben die kleiner is dan 150 mm. Een belangrijke voorwaarde is daarbij wel dat de opening door buigen - met mankracht - niet makkelijk is te vergroten. Met andere woorden dat de staven van traliewerk e.d. niet makkelijk zijn te verbuigen. Hierbij is het tevens van belang dat de aangebrachte voorzieningen niet makkelijk vanaf de buitenzijde zijn te verwijderen en dat de bevestiging voldoende stevigheid biedt.

Er bestaan geen separate richtlijnen om het hiervoor genoemde te beoordelen, zodat de beoordeling dient plaats te vinden op basis van de vereiste inbraakvertraging volgens de bouwkundige niveaus B1, B2 en B3 en document 002757 augustus 2001 versie 2: Installatievoorschriften voor rolluiken, rolhekken en schaarhekken, en in document D03/394 september 2003 versie 2: Inbraakwerende beglazing; hoofdstuk 4 'producten om glas af te scherpen'

4 Elektronische maatregelen

In de tabellen van de beveiligingsklasse voor woningen en bedrijven worden de vereiste elektronische maatregelen aangeduid met de letter E en een letter of cijfer. De toevoeging achter de 'E' heeft betrekking op omvang en het niveau van deze maatregelen.

4.1 Omvang van de Elektronische maatregelen

In het op te stellen beveiligingsplan dient te worden bepaald welke typen detectoren in welke ruimten en op welke plaatsen moeten worden aangebracht. De zwaartepunten in het beveiligingsplan worden hierbij gevormd door de plaatsen waar zich de attractieve goederen bevinden. Bij het opstellen van het beveiligingsplan zal echter ook nagegaan moeten worden welke andere - eventueel verbindende - ruimten in het bewaakte gebied moeten worden opgenomen.

Uit het voorgaande volgt dat het bewaakte gebied zich niet alleen beperkt tot ruimten op de begane grond, maar zich in bepaalde gevallen ook uitstrekt tot ruimten in de kelder of op de verdiepingen. Dit zijn in principe alle ruimten die voor een inbreker bereikbaar zijn vanaf het openbare gebied. Het voorgaande betekent tevens dat bepaalde ruimten niet tot het bewaakte gebied gerekend behoeven te worden. Dit betreft bijvoorbeeld een toiletruimte op de begane grond met een ventilatieaampje met een dagmaat van minder dan 15 cm. Daarnaast kunnen ook andere ruimten van het bewaakte gebied worden uitgezonderd indien dit in overeenstemming is met de verdere invulling van het beveiligingsplan.

4.2 Ontwerp en aanleg

De alarminstallatie dient te worden ontworpen, aangelegd en onderhouden volgens de Installatievoorschriften voor alarmapparatuur document 002080 juli 2000 versie 2 en de Voorschriften beheer en onderhoud alarmapparatuur document 002079 juli 2000 versie 2.

Voor de detectie dient gebruik gemaakt te worden van een - op het risico afgestemde - combinatie van ruimtelijke - en omtrek detectie. De status van het systeem in het beveiligde object moet steeds afleesbaar zijn. Bij toepassing van mistgeneratoren is bijlage 2 van document D01/026 oktober 2001 versie 2 van toepassing

4.3 Het niveau van de Elektronische maatregelen

Hierna volgen de omschrijvingen van de eisen waaraan de elektronische maatregelen moeten voldoen. Alarmering: Zodra de alarminstallatie in alarm komt - dat wil zeggen dat één of meer detectoren in het bewaakte gebied de alarmstatus bereiken - dient er een alarmering plaats te vinden. De eisen daaraan zijn opgenomen in hoofdstuk 6: "Alarmering" in dit document.

4.3.1 Ed niveau

Inleiding: aan de basis van de elektronische inbraaksignaleringsystemen voor woningen staat het E1 niveau. Dit E1 niveau dient altijd op een erkende BORG Particuliere Alarmcentrale (PAC) te worden aangesloten. In bepaalde gevallen kunnen er voor gebruikers en verzekeraars redenen zijn om genoeg te nemen met een inbraaksignaleringsstelsel zonder aansluiting op een PAC. Zij wensen echter wel de zekerheid dat de installatie uit goede componenten bestaat en deskundig is aangelegd. Bovendien willen zij graag dat aansluiting op een PAC in een later stadium altijd mogelijk blijft. Dit Ed niveau, **wat uitsluitend geldt voor woningen** in risicoklasse 1, is Ed genoemd. De 'd' staat daarbij voor domestic oftewel woonhuizen.

Eisen:

Het BORG Beveiligingsbedrijf en de BORG Alarminstallateur zijn verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006 en NEN-EN 50136 of Technische Specificaties (TS'n). Van toepassing is security grade 2 / Klasse 2 (zie toelichting bij 4.3.5) Uitzondering hierop is dat de optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn. Inbraaksignaleringsstelsel op het niveau Ed mogen ook volledig draadloos of gedeeltelijk draadloos worden aangelegd. Voor de alarmering is het niveau AL 0 van toepassing. De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per 2 jaar. Extra eisen bij toepassing van draadloze systemen: (zie niveau E1 eisen aan draadloze systemen)

Omvang projectie minimale eisen:

Voor alarmgevers en alarmtransmissie zie niveau AL0. Voor de alarmopvolging zie niveau R0
Indien een alarminstallatie van niveau Ed wordt aangesloten op een PAC moet worden voldaan aan de eisen onder E1, AL1 en R1.

4.3.2 E1 niveau

Het BORG Beveiligingsbedrijf en de BORG Alarminstallateur zijn verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006 en NEN-EN 50136 of Technische Specificaties (TS'n). Van toepassing is security grade 2 / Klasse 2 (zie toelichting bij 4.3.5) Uitzonderingen hierop zijn: de alarmtransmissie-inrichting moet zijn voorzien zijn van een CE goedkeuring en een conformiteitsverklaring voor het aansluiten en toepassen op communicatie infrastructuur en netwerken.

Optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn. Inbraaksignaleringsstelsel op het niveau E1 mogen ook draadloos worden aangelegd en dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Extra eisen bij toepassing van draadloze alarmapparatuur:

1. Bij aansluiting op een PAC is doormelding van de beheers (supervisie)- en communicatiemeldingen (jamming) verplicht. De PAC moet op deze meldingen van een geactiveerd systeem reageren als bij een sabotagemelding. Het opnemen in computer log-files en achteraf rapporteren aan installateur is onvoldoende. Er dient een schriftelijke overeenkomst met gebruiker en/of installateur te zijn, waarin is vastgelegd dat deze meldingen zo spoedig mogelijk aan klant en/of installateur worden doorgegeven, zodat adequate maatregelen getroffen kunnen worden.
2. De frequentie van onderhoud moet mede zijn gebaseerd op de levensduur/gebruiksduur van de batterijen met een minimum van één keer per jaar. De periode dat een batterij meegaat moet worden bepaald aan de hand van te verwachten activeringen. Batterijen moeten van het door de fabrikant voorgeschreven type zijn. Een batterij "laag" signaal dient vooraf door het systeem lokaal te worden aangegeven. Indien de batterij niet tijdig wordt vervangen dient dit als laatste naar de PAC worden doorgegeven. Bij geen daadwerkelijke vervanging zal dit dan uiteindelijk leiden tot een zenderverlies signaal (1)

tabel 1

Woningen	Ed	E1	E2	E3
Volledig bedrade systemen	ja	ja	ja	ja
Draadloze systemen	ja	ja	nee	nee

Bedrijven	E1	E2	E3
Volledig bedrade systemen	ja	ja	ja
Draadloze systemen	ja/nee*	nee	nee

* wel in risicoklasse 1 en niet in risicoklasse 2, 3 en 4

Omvang projectie minimale eisen:

Ruimte detectie op plaatsen waar zich de attractieve goederen concentreren en op strategische plaatsen in het pand voor vroegtijdige detectie. Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt. Ruimte detectie ter plaatse van bediendelen.

Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembepurende maatregelen zijn toegepast.

Openstand detectie op de entree deur(en) en nooduitgangen van het pand.

Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.

Openstand detectie op deuren van waardebergingen (compartimenten)

Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet altijd in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Voor de alarmering is het AL1 traject van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie mei 2007 of D03/376 (bedrijven) versie mei 2007.

4.3.3 E2 niveau

Het BORG Beveiligingsbedrijf en de BORG Alarminstallateur zijn verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006 en NEN-EN 50136 of Technische Specificaties (TS'n). Van toepassing is security grade 2 of 3 / Klasse 2 of 3 (zie toelichting bij 4.3.5)

Uitzonderingen hierop zijn: de alarmtransmissie-inrichting moet zijn voorzien van een CE goedkeuring en van een conformiteitsverklaring voor het aansluiten en toepassen op communicatie infrastructuren en netwerken

Optische alarmgevers (flitsers) mogen worden toegepast die niet gecertificeerd zijn.

Inbraaksignaleringsstelsel op het niveau E2 mogen ook draadloos worden aangelegd met de beperkingen genoemd in tabel 1 in artikel 4.3.2

Ruimtelijk werkende detectoren zijn van het type anti-masking. Voor woningen is dit geen eis.

De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Omvang projectie minimale eisen:

Ruimte detectie op plaatsen waar zich de attractieve goederen concentreren en op strategische plaatsen in het pand voor vroegtijdige detectie. Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt. Ruimte detectie ter plaatse van bediendelen.

Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembepurende maatregelen zijn toegepast.

Openstand detectie op de voor inbrekers bereikbare gevelopeningen (ramen en deuren in de buitenschil van het pand, mits niet afgeschermd) voor de bereikbaarheid geldt de NEN 5087. Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.

Openstand detectie op deuren van waardebergingen (compartimenten)

Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Schildetectie niveau 2: bij bedrijven in risicoklasse 3 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie en alarmering bij eerste aanval op bereikbare vaste en beweegbare gevelelementen die direct toegang geven tot de ruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d. Meetstaf bereikbaarheid gevelelementen is de NEN 5087

Voor de alarmering is het AL1 of AL2 traject van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie mei 2007 of D03/376 (bedrijven) versie mei 2007.

4.3.4 E3 niveau

Het BORG Beveiligingsbedrijf en de BORG Alarminstallateur zijn verplicht gebruik te maken van gecertificeerde componenten die voldoen aan de Europese NEN-EN 50131-1:2006 en NEN-EN 50136 of Technische Specificaties (TS'n). Van toepassing is security grade 3 / Klasse 3 (zie toelichting bij 4.3.5) Uitzondering is: de alarmtransmissie-inrichting moet zijn voorzien van de CE goedkeuring en van een conformiteitsverklaring voor het aansluiten en toepassen op communicatie infrastructuren en netwerken.

Ruimtelijk werkende detectoren zijn van het type anti-masking.

Voor de alarmering is het niveau AL2 of AL3 van toepassing, zie tabellen risicoklasse / beveiligingsklasse in documenten D03/375 en D03/376 versie mei 2007.

De alarminstallatie dient te worden onderhouden en in overeenstemming te blijven met het niveau van het oorspronkelijke beveiligingsplan. Voor de controle hierop moet een onderhoudscontract worden afgesloten, dat voorziet in ten minste één onderhoudsbeurt per jaar.

Omvang projectie minimale eisen:

Ruimte detectie op plaatsen waar zich de attractieve goederen bevinden en op strategische plaatsen in het pand voor vroegtijdige detectie. Ruimte detectie voordat de CCS, en daartoe behorende delen, kunnen worden bereikt. Ruimte detectie ter plaatse van bediendelen.

Ruimte detectie in ruimten met een waardeberging (safe) of wanneer daar meeneembepaalde maatregelen zijn toegepast. Openstand detectie op de voor inbrekers bereikbare gevelopeningen (ramen en deuren in de buitenschil van het pand, mits niet afgeschermd). Voor de bereikbaarheid geldt de NEN 5087.

Openstand detectie op rolluiken, rolhekken en schaarhekken met een beveiligingsfunctie.

Openstand detectie op deuren van waardebergingen (compartimenten)

Openstand detectie op de deur waarachter de CCS is opgesteld (meterkast)

Noot: Bij woningen kan het voorkomen dat de CCS niet in de meterkast wordt geplaatst.

Bij bedrijven is het plaatsen van de CCS in een afgesloten ruimte wel een eis.

Schildetectie niveau 2: bij bedrijven in risicoklasse 4 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie en alarmering bij eerste aanval op bereikbare vaste en beweegbare gevelelementen die direct toegang geven tot de ruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d. Maatstaf bereikbaarheid gevelelementen is de NEN 5087

Schildetectie niveau 3: bij bedrijven met de omschrijving attractieve goederen in magazijn in bijlage 1 van document D03/376 waar geen C/M maatregelen worden getroffen geldt als extra eis: detectie bij eerste aanval op bereikbare vaste en beweegbare gevelelementen, gevels, vloeren, daken en scheidingsconstructies die direct toegang geven tot de opslagruimten met de attractieve goederen.

Voorbeelden van detectiemethoden: glasbreukdetectie / trillingsdetectie / video bewaking met motion detectie / buitendetectie / inpandige ruimtedetectie aan de aanvalszijden e.d.

Maatstaf bereikbaarheid gevelelementen, gevels, vloeren en daken is de NEN 5087

Voor de alarmering is het niveau AL2 of AL3 van toepassing, zie hiervoor de tabellen van de gekozen risicoklasse en beveiligingsklasse in document D03/375 (woningen) versie mei 2007 of D03/376 (bedrijven) versie mei 2007

4.3.5 Eisen aan alarmapparatuur:

De toegepaste componenten dienen te voldoen aan de eisen van de NEN-EN 50131-1:2006 en NEN-EN 50136 of Technische Specificaties (TS'n) Dit kan worden aangetoond door het overleggen van het productcertificaat, afgegeven door een voor het betreffende toepassingsgebied geaccrediteerde certificatie-instelling die tevens volledig lid is van de EA, of een verwijzing naar de lijst geregistreerde producten van de stichting REQ (Registration European Quality mark) en/of EQM Tot 1-1-2012 kan aan bovengenoemde eis ook worden voldaan door gebruik te maken van alarmapparatuur waarvoor een productcertificaat is afgegeven op basis een nationale norm, technische specificatie of productrichtlijn zoals bijvoorbeeld ANPI, Certec, VDS (klasse B=2 of C=3), NFA2P, IMQ vanaf klasse 2, etc. In de REQ lijst 'Overige producten' en de lijst NCP registratie wordt een overzicht gegeven van deze producten.

Toelichting: Componenten voor alarmapparatuur zijn (nog) niet allemaal getest volgens de NEN-EN normen. Doelstelling is dat op uiterlijk 1-1-2012 voldoende componenten voor alarmapparatuur beschikbaar zijn met een (REQ/EQM) registratienummer.

In geval dat er in Nederland geen componenten beschikbaar zijn die voldoen aan de security grade of klasse voor het betreffende niveau kan gebruik worden gemaakt van componenten met een lagere security grade of klasse. Wanneer ook die ontbreken dient u zelf, op basis van goed vakmanschap, te bepalen of het product voldoet aan de duurzaamheid en functionele eisen die u hieraan stelt. Vermeldt afwijking op dit onderdeel in het PvE en het beveiligingsplan.

Het begrip Grade:

Security Grades: binnen de EN50131 / 50136 serie wordt uitgegaan van het niveau van de aanvaller (Inbreker / Overvaller)

Grade 1: (laag risico) Verwacht wordt dat aanvallers weinig kennis hebben van inbraak/overval detectiesystemen, en is gelimiteerd tot een beperkte set standaard gereedschappen. Ter indicatie VDS klasse A (geen sabotage circuit) Deze grade kan overeenkomen met de doe het zelf markt.

Grade 2: (laag tot gemiddeld risico) Verwacht wordt dat aanvallers gelimiteerde kennis hebben van inbraak/overval detectiesystemen en van vrij verkrijgbare gereedschappen en draagbare apparatuur waaronder o.a. multimeter.) Ter indicatie: ANPI, Certec, VDS klasse B. Deze grade kan overeenkomen met de particuliere markt.

Grade 3: (gemiddeld tot hoog risico). Verwacht wordt dat aanvallers bekend zijn met inbraak/overval detectiesystemen en hebben een uitgebreide set gereedschappen en draagbare elektronische (meet)apparatuur. Deze grade kan gelden voor high-end particuliere markt, winkels en bedrijven.

Ter indicatie: ANPI, Certec, VDS klasse B en C

Grade 4: (hoog risico) Wanneer beveiliging voorrang heeft op alle andere factoren. Verwacht wordt dat aanvallers de middelen of vermogen hebben een inbraak tot in detail voor te bereiden en de beschikking hebben over een volledige set gereedschappen/ apparatuur inclusief mogelijkheden om vitale componenten van het inbraak/overval detectiesysteem te substitueren. Ter indicatie: VDS klasse C (Grade 4 kan gelden voor hoge risico's)

Environmental classes: binnen de EN5013x wordt uitgegaan van het niveau van de aanvaller.

Class 1: (Binnen) Temperatuur goed geregeld, bijvoorbeeld particulier of kantoor.
(Temp: + 5C <-> + 40C, Rel. vochtigheid: 75%, niet condenserend)

Class 2: (Binnen generiek) Temperatuur minder goed geregeld, bijvoorbeeld onverwarmde magazijnen, gangen en trappenhuisen.
(Temp: - 10C <-> + 40C, Rel. vochtigheid: 75%, niet condenserend)

Class 3: (Buiten afgeschermd) Het product wordt blootgesteld aan buitentemperaturen, maar wordt is afgeschermd en wordt niet volledig blootgesteld aan het weer.
(Temp: - 25C <-> + 50C, Rel. vochtigheid: 75%, [30d] 85% <-> 95%, niet condenserend)

Class 4: (Buiten generiek) Het product wordt buiten volledig blootgesteld aan weer en wind.
(Temp: - 25C <-> + 60C, Rel. vochtigheid: 75%, [30d] 85% <-> 95%, niet condenserend)

4.3.6 Brandpreventie (brand) rookmelders.

In het Bouwbesluit 2003-artikel 2.146 worden niet ioniserende rookmelders met secundaire energievoorziening, aangesloten op het lichtnet, voor nieuwbouwwoningen en woningrenovatie verplicht gesteld (samengevat: gebouwen met een woonfunctie). Deze huisrookmelders moeten voldoen aan EN 14604 - NEN 2555. Voor bestaande woningen kan volstaan worden met rookmelder(s) met batterijvoeding. (Hier mogen ook rookmelder(s) met secundaire energievoorziening, aangesloten op het lichtnet worden toegepast). Ook de rookmelder voor bestaande woningen moet voldoen aan EN14604. Beide typen rookmelders moeten voorzien zijn van het KOMO keur. Van toepassing is: bewoners dienen ingeval van rookontwikkeling tijdig gealarmeerd te worden door middel van een akoestisch signaal, waardoor de tijd om maatregelen te nemen en/of te vluchten aanzienlijk kan worden vergroot.

Maatregelen: In gebouwen met woonfuncties moeten in de verkeersruimten één of meerdere rookmelders geplaatst worden. Verkeersruimten zijn die ruimten waarop verblijfsruimten uitkomen; verkeersruimten zijn doorgangsruidten die zich op alle verdiepingen in een woning bevindt (vluchtwegen) Voor projectering / plaatsing wordt verwezen naar het Bouwbesluit 2003- artikel 2.146 en NEN 2555- artikel 7. Hierbij gaat de voorkeur uit naar rookmelders met een secundaire energievoorziening die zijn aangesloten op het lichtnet. Hier mogen ook rookmelders met batterij voeding worden aangebracht.

Ter verhoging van de veiligheid wordt aangeraden de rookmelders onderling te koppelen. Installatie van rookmelders aangesloten op het lichtnet moet volgens de geldende voorschriften voor elektrotechnische installaties gedaan worden (NEN 1010).Daarnaast gelden de montagevoorschriften van de leverancier die bij elke rookmelder meegeleverd wordt. De gebruiksaanwijzing van de rookmelder moet, t.b.v. de bewoners, in de woning achtergelaten worden. Regelmatig dient de bewoner te controleren of de rookmelder nog naar behoren werkt. Door de testknop op de rookmelder in te drukken worden de functie van de rookmelder (en rookmelders in het geval deze gekoppeld zijn) getest. Bij doven en slechthorende bewoners is het zeer aan te bevelen een optische signalering aan te brengen en een trilwekker onder het kussen. Eenvoudige blusmiddelen kunnen als aanvullend advies worden opgenomen.

Aanbevelingen: het is toegestaan een rookmelder aan te sluiten op een alarminstallatie, mits er sprake is van aansluiting op een aparte 24-uurs groep van de Centrale Controle- en Sturingseenheid (CCS). De rookmelder(s) kunnen d.m.v. een potentiaalvrij contact op een dergelijke alarminstallatie aangesloten worden mits er geen wettelijke bepalingen zijn om een ontruimingsinstallatie in het gebouw aan te brengen. Anders wordt verwezen naar de wettelijke bepalingen volgens NEN-EN 2535 en NEN-EN 2575.

Indien er sprake is van een onveilige situatie dient het specifieke signaal als zodanig herkenbaar bij de Particuliere Alarm Centrale (PAC) binnen te komen. Hierbij moet rekening worden gehouden met voorschriften van de alarmopvolgers. Dit betekent dat voor brandmelders aangesloten op een inbraakalarminstallatie ook altijd alarmverificatie moet plaatsvinden voordat de brandweer door de PAC, naar de woning mag worden gestuurd.

Bij bedrijven is branddetectie een apart aandachtsgebied en in de gebruiksvergunning mogelijk een eis. In dat geval verwijzen we naar de BORG regeling Brandmeldinstallaties, NEN-EN 2535 en NEN-EN 2575. Daar waar deze eisen niet van toepassing zijn, kan het aanbrengen van enkele brandmelders (rookmelders) op vitale plaatsen in het bedrijf zinvol zijn. Deze mogen onder voorwaarden worden aangesloten op het inbraaksignaleringssysteem.

Van toepassing is: additionele toepassingen zoals brand-, overval-, kluis- en technische alarmen mogen alleen op een aparte groep worden aangesloten op de CCS. De ontstane onveilige situaties worden als afzonderlijk herkenbare meldingen doorgemeld naar de PAC. **Hierbij moet rekening worden gehouden met voorschriften van de alarmopvolgers.** Dit betekent dat voor brandmelders aangesloten op een inbraakalarminstallatie ook altijd alarmverificatie moet plaatsvinden voordat de brandweer door de PAC, naar het object mag worden gestuurd. Zowel bij woningen als bedrijven geldt dat deze additionele toepassingen de goede werking van de alarmapparatuur nimmer nadelig zal beïnvloeden. Het brandalarm en het inbraaksignaleringssysteem mogen niet van hetzelfde akoestische signaal gebruik maken. Voor een rook/brandalarm wordt gebruik gemaakt van een zogenaamd slow-whoop-signaal

4.3.7 Beveiligingsverlichting

Voor woningen is in het bouwbesluit en het Politie Keurmerk Veilig Wonen beveiligingsverlichting verplicht gesteld. Van toepassing is:

Bereikbare deuren van een woning, die vanuit openbaar gebied of andere woningen zichtbaar zijn. Deze dienen zodanig te zijn verlicht dat de bezoekers en bewoners bij schemer of donker in het licht staan.

Maatregelen:

Bij achter- en zijdeuren op de begane grond is een buitenlamp aangebracht. Bij (balkon)deuren op de eerste verdieping is een buitenlamp aangebracht, indien deze door opklimming bereikbaar is en er op de begane grond geen verlichting is.

Indien de voordeur van de woning in een portiek, nis of onder een overkapping is gelegen, is een buitenlamp aangebracht. Als er meer deuren in hetzelfde gevelvlak aanwezig zijn, kan worden gekozen voor een centraal aangebrachte buitenlamp, mits de lichtval op de deuren niet wordt onderbroken door verspringingen op of in de gevel.

Indien er sprake is van voldoende openbare verlichting ter plaatse van de bereikbare deuren is deze beveiligingsrichtlijn niet van toepassing.

De voorkeur gaat uit naar een vandalismebestendig armatuur (slagvaste kap en buiten bereik aangebracht) met schemerschakelaar, bewegingssensor of tijdschakelaar.

Installatie volgens de NEN1010 en de voorschriften van het gecontracteerde Energiebedrijf. Daarnaast gelden de bijgeleverde montagevoorschriften van de leverancier.

Toelichting:

Deze beveiligingsrichtlijn is zowel van toepassing op deuren op de begane grond van (flat)woningen als op (balkon)deuren op de eerste verdieping, indien deze door opklimming bereikbaar zijn. Zie voor een toelichting ook de NEN 5087.

Aanbevelingen:

Verlichting bij de voordeur op begane grond alsook op de galerij, geeft een verhoging van de sociale veiligheid. Bezoekers zijn duidelijk zichtbaar en herkenbaar, zowel vanuit de woning als vanuit de omgeving. Aanwezige struiken en bomen mogen de lichtval niet hinderen.

Indien de afstand tussen achter- of zijgevel van de woning en een aanwezige schuur, garage of berging beperkt is, kan een eventueel aanwezige buitenlamp op de gevel van deze bijgebouwen voldoende licht werpen op de deur. De hoogte waarop de buitenlampen op de gevel van de woning en/of bijgebouwen bij voorkeur worden opgehangen is 2,7 meter. Verlichtingssterkte is minimaal 10 lux.

Bij bedrijven is beveiligingsverlichting een apart aandachtsgebied. Een inbreker wordt niet graag gezien. Beveiligingsverlichting langs de buitenkant van het gebouw werkt preventief. Tenminste, indien de omgeving (sociale) controle toelaat en de inbreker inderdaad de kans loopt om gezien te worden. Aandachtpunten zijn:

Wat is het doel van de verlichting? Sociale controle, preventie, beveiliging, cameratoezicht e.d.
Lichtreflectie-eigenschappen omgeving, hoeveelheid licht, kleur van het licht, kleurweergave index Ra waarde. Plaats en type van de lichtbron, soorten armaturen, energieverbruik, levensduur van lampen, wijze van in - uitschakelen, lichthinder, milieu en gezondheid, onderhoud e.d.
In een goed beveiligingsplan is de beveiligingsverlichting een belangrijk onderwerp.
Van toepassing is de NEN 1010 en aanwijzingen van de leverancier van het product.

4.3.8 Camerasystemen

Camerasystemen spelen een steeds belangrijk wordende rol bij preventie.

In relatie tot de preventiewaarde kan een onderscheid worden gemaakt tussen camerasystemen waarvan de beelden binnen het bedrijfspannend kunnen worden weergegeven. Denk aan overval preventie in winkels en toezicht op vitale plaatsen in het bedrijf

Er kan sprake zijn van beeldopslag en/of dat de camerabeelden worden verzonden naar een centraal punt PAC of service centrale.

Camerasebeelden kunnen ook worden aangewend bij alarmverificatie.

Gebruik van videocameratoezicht (CCTV) is aan veel richtlijnen en wettelijke (ook Europese) regels gebonden. We noemen er slechts enkele zoals de Wet bescherming persoonsgegevens en de Wet heimelijk cameratoezicht. Een werkgroep buigt zich momenteel over de invulling van de technische - en procedurele eisen waaraan camerasystemen voor alarmverificatie moeten voldoen. Dit onderdeel wordt nog ingevuld in dit document en de installatievoorschriften voor alarmapparatuur.

4.3.9 Toegangscontrole

Toegangscontrolesystemen en terreinafscheidingen (hekwerven)

Uitvoeringsnormen zoals bij inbraakbeveiliging zijn in Nederland niet beschikbaar.

Voor toegangscontrolesystemen geldt: de NEN-EN 50133 deel 1 t/m 7, CE aantekening van de fabrikant en RDR nummer voor RF apparatuur. Er zijn classificaties voor systemen (A, B en Ba) en voor toegangscontrole lezers (klasse 0 t/m 3)

Bij terreinafscheidingen gaat het om een substantiële belemmering voor inbrekers om het terrein te betreden. De preventiewaarde neemt toe naarmate deze afscheidingen zijn voorzien van schrikdraad, detectie tegen door - of overklimmen en sabotage.

4.3.10 Buitendetectie

Bij deze detectiemiddelen gaat het om systemen die het betreden van terreinen door personen of voertuigen detecteert. We onderscheiden E-veld systemen, schrikdraad gekoppeld aan detectie, drukdetectie, trillingsdetectie, magneetcontacten, actief infrarood, passief infrarood, radar, video-motion e.d. Het doel is: afschrikken, detecteren, vertragen, actie ondernemen en toegang verschaffen. Buitendetectie systemen vragen altijd alarmverificatie, in combinatie met bijvoorbeeld alarmgestuurde dome-video-camera's bieden deze maatregelen een goede oplossing. De klimatologische omstandigheden waaronder deze systemen functioneren zijn niet te vergelijken met geveldetectie of ruimte detectie in een gebouw.

5. Compartimentering en Meeneembepurende maatregelen (C/M)

5.1 Inleiding

Een nog steeds groeiend aantal inbraken en diefstallen bij bedrijven en particulieren noopt tot het nemen van preventieve maatregelen. Inventarisatie van schadecijfers en modus operandi leiden tot de volgende stelling: inbraak - en diefstalpreventie blijft een absolute noodzaak, waarbij de aanpak met name dient te worden bezien vanuit de positie van de crimineel. Ofwel: welke voorziening sorteert het beste effect om een inbreker te slim af te zijn? Het is daarbij de kunst om de zichtbare drempel voor de inbreker zo hoog te leggen, dat het voor hem niet de moeite loont een inbraak - of diefstalpoging te ondernemen. Ondanks soms uitgebreide preventieve maatregelen, worden goederen toch gestolen; vaak binnen een zeer kort tijdsbestek, de zogenaamde 'snelkraak'. Na het doorbreken van de bouwkundige schil van een gebouw (via raam, deur of wand) is de inbreker in staat om binnen zeer korte tijd voldoende waardevolle goederen te stelen om de inbraak 'lonend' te maken. Dit gebeurt ondanks de aanwezige alarmering, omstanders of bewoners. Dat dit de praktijk is, blijkt uit de volgende redenen:

- de schil van een gebouw is zelden voorzien van elektronische detectie, waardoor er tot het moment van binnenkomst geen alarm zal zijn (er is dus vaak veel tijd om in te breken),
- de buitenzijde van een gebouw is veelal bouwkundig - door de omvang - moeilijk haalbaar inbraakvertragend te maken. Bovendien kunnen daders in alle rust (ontbreken van sociale controle) en met gebruik van zware inbrekersgereedschappen hun gang gaan. Buitendetectie om het gebouw is een zeldzaamheid,
- nadat men is binnengedrongen bestaan er, in pandig, doorgaans nauwelijks vertragingen meer,
- de inbreker weet dat een elektronisch alarm niet direct tot alarmopvolging leidt en dat hij vaak tien tot vijftien minuten de tijd heeft om goederen van zijn gading te vergaren. De praktijk wijst op aanrijtijden van een half uur of langer,
- de inbreker weet vaak, door een gedegen voorkennis, waar de bewuste goederen zich bevinden,
- attractieve goederen zijn veelal niet erg volumineus, waardoor er in een kort tijdsbestek goederen zijn te verzamelen en er snel sprake is van een relatief grote buit,
- de meeste attractieve goederen liggen vaak, vanwege de commercie, vóór in de winkel en/of aantrekkelijk uitgesteld voor het publiek. Dus meestal zó voor het grijpen,
- inbrekers worden steeds brutaler en lijken zich vaak niet te storen aan getuigen en/of omstanders in een alarmfase, sterker nog, deze worden nog al eens bedreigd.

5.2 Attractieve goederen

Goederen zijn pas écht attractief als deze snel vervoerbaar, goed verhandelbaar en zonder directe pakkans voor de crimineel kunnen worden verkregen. De afzet en het transport ervan zijn, door voorkennis en inventiviteit vooraf, goed geregeld. Hoe groter de buit, hoe slimmer het 'gilde'! Als het gaat om attractieve goederen zijn er drie situaties te onderscheiden, nl.;

- goederen voor eigen gebruik,
- verkoopgoederen in winkel en showroom
- goederen in opslag of in magazijn.

Voor een goed functioneren van alle meeneembeperkende maatregelen is een deugdelijke en tegen sabotage beveiligde alarminstallatie een voorwaarde. Samen met het direct ter plaatse ontstane optisch- en akoestisch signaal + de doormelding én de alarmopvolging kunnen we het gedrag van de crimineel dusdanig beïnvloeden dat de kans op diefstal van de attractieve goederen kleiner wordt. Onderstaand worden in dit verband voor de drie situaties een paar voorbeelden gegeven bij een 9-tal symbolische pictogrammen. In feite moet men, door inventief te zijn en door rekening te houden met de meest geschikte materialen, zelf de beste aanpak bepalen. Om in showrooms en binnen kantoren een esthetisch verantwoorde voorziening te maken, kan gebruik worden gemaakt van inbraakwerende materialen als polycarbonaat, hout, geplastificeerd of gespoten traliewerk, roestvrij staal enz. Standaardvoorzieningen zijn verkrijgbaar om computers en randapparatuur te verankeren aan wand, vloer of bureau.

Veel standaard materialen en bouwkundige voorzieningen, zoals bijvoorbeeld stalen rolluiken, kunnen ook worden toegepast in binnensituaties. Stalen zee-containers kunnen dienst doen als -, c.q. binnen magazijn, of opslag.

Ook met alleen organisatorische maatregelen kan soms al een goed effect worden verkregen, immers door de attractieve goederen te verstoppen, zal het zoeken ernaar, in een alarmfase, te veel tijd vergen.

De verdere invulling en concretisering zijn aan de beveiligingsadviseur en de gebruiker zelf, waarbij rekening zal moeten worden gehouden met situering, materiaalsoort en -sterkte, esthetische eisen, bedieningsgemak en kosten. Tijdelijke en/of 'mobiele' voorzieningen vragen om veel discipline en organisatie, waarbij diverse handelingen elke keer bij winkelsluiting terugkeren en als hinderlijk kunnen worden ervaren. Daardoor is het gevaar groot dat men ze, zeker na verloop van tijd, achterwege zal laten en het meeneembeperkende effect nihil wordt. Heel essentieel is het effect van een bouwkundige barrière of voorziening binnen een elektronisch beveiligd gebied met een zeer deugdelijke en goed zichtbare preventieve uitstraling.

5.3 Normstelling

De enige norm die hier in feite telt is het tijdsbestek wat men wint door de toepassing van een goede meeneembeperkende maatregel nadat een elektronisch alarm is afgegaan.

Inventiviteit is hier troef, immers een potentiële inbreker komt overdag eerst kijken hoe het met alle maatregelen tegen inbraak gesteld is. Indien de genomen maatregelen overtuigend genoeg zijn, zullen deze maar zelden op hun sterkte worden beproefd opdat, als gezegd, ook inbraakpogingen waarschijnlijk achterwege zullen blijven. Afhankelijk van de duur van een alarmopvolging (in tijd gemeten) moet een oplossing voor de attractieve goederen of artikelen worden bedacht. Het gebruik van sterk materiaal, zwaar hang- en sluitwerk is uiteraard een eerste vereiste (zie BRL 3104 hang- en sluitwerk en BRL 9904 hangsloten), waarbij vooral de onderlinge samenhang van de toegepaste materialen telt. Tot slot kan elke functionele meeneembeperkende maatregel individueel tot norm worden verheven als blijkt dat het voor een inbreker niet de moeite loont eraan te beginnen tijdens een alarmfase.

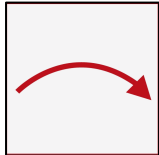
5.4 Conclusie

Slechts enkele standaard oplossingen zijn hier aan te dragen, zodat met betrekking tot dit onderwerp een beroep wordt gedaan op het inlevingsvermogen van iedere adviseur, ondernemer of particulier. Een effectieve meeneembeperkende maatregel zal zelden op zijn sterkte worden beproefd, immers een inbreker ziet (overdag reeds) waar hij tijdens een elektronisch alarm aan moet gaan beginnen. Inventiviteit blijft troef, waarbij de keuze voor materialen, vormgeving, opstelling en samenhang voor elke oplossing weer anders kan zijn. De mogelijkheden van vormgeving, uiterlijk, materiaaltoepassing en gebruikersgemak zijn legio, waardoor in feite voor elke situatie een meeneembeperkende maatregel kan worden bedacht. Het zijn het inzicht in de materie en de wil om op deze manier inspanning te geven die hierbij de doorslag geven. Veel goede oplossingen zijn inmiddels op een inventieve en creatieve manier gerealiseerd.

5.5 Pictogrammen, uitleg en voorbeelden

Op de volgende pagina's zijn negen pictogrammen afgebeeld en situaties beschreven voor de toepassing van meeneembeperkende maatregelen.

5.6 C/M 1 niveau prestatie-eis 3 minuten inbraakvertraging



5.6.1 Verplaatsen

Eigen gebruik

Een verstopt artikel is moeilijk en niet snel vindbaar na een elektronische alarmering!

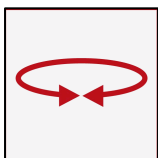
Winkel of showroom

Door het gebruik van een kelder- of bovenverdieping voor het etaleren van duurdere goederen is de weg naar deze goederen toe vaak te lang na het activeren van het elektronisch alarm. Ook de afvoer van de goederen neemt immers meer tijd in beslag. Deze oplossing is bepaald niet 'zaligmakend' en dient uitsluitend voor enkele kleinere gevallen, omdat de praktijk ook uitwijst dat het 'gilde' vaak zeer brutaal is en/of met meer personen tegelijk veel aandurft en veel aankan in een zeer kort tijdsbestek

Magazijn of opslag

Door attractieve goederen hoog in de stellingen te plaatsen, ontstaat een grote handicap voor de inbreker, hij moet immers over een heftruck beschikken om de goederen naar beneden te halen. Binnen een elektronisch beveiligd gebied is dit bijna een onmogelijkheid. Wél is het zaak om de heftruck na sluitingstijd onklaar te maken! Niet zelden komt het voor dat de crimineel het eigen expeditievoertuig, welke soms al geladen staat met attractieve goederen, gebruikt voor de afvoer.

Meeneembeperkende maatregelen dienen dus niet alleen te worden toegepast op het product maar ook op bedrijfsmiddelen en gereedschappen die kunnen worden gebruikt voor het verbreken, verzamelen en vervoeren. Hiermee vergelijkbaar is de opslag op een entresol, waarbij het essentieel is dat een trap niet een, twee, drie de mogelijkheid biedt om boven te komen na inbraak.



5.6.2 Koppelen

Eigen gebruik

Een PC unit kan door middel van een stalen (standaard) kabel worden gekoppeld aan een bureau. Ook de steeds vaker voorkomende flatscreens in kantoren zijn op deze manier minder interessant te maken voor diefstal. Zie hiervoor de aanbevelingen

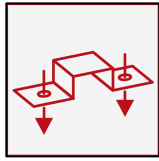
Meeneembeperkende Producten op basis van SKG-KE 470 augustus 2005

Winkel of showroom

Door duurdere fietsen, scooters of bromfietsen onderling te koppelen met beugelsloten (eigen verkoop) en/of geplastificeerde staalkabels wordt snelkraak voorkomen. Een goed zichtbare drempel werkt op deze manier met name in een dagsituatie zeer preventief. De inbreker weet in dit geval dat hij na een elektronisch alarm nog met een volgend probleem te kampen krijgt!

Magazijn of opslag

Niet verpakte en grotere vaak verrijdbare handelsgoederen in magazijnen kunnen onderling met zwaardere geplastificeerde kabels onderling worden gekoppeld. Bijvoorbeeld onderling gekoppelde aanhangwagens of aggregaten zijn moeilijk snel aan te koppelen en mee te nemen. Indien dit binnen een elektronisch beveiligd gebied gebeurd is diefstal vrijwel onmogelijk binnen het tijdsbestek van de alarmopvolging.



5.6.3 Verankeren

Eigen gebruik Een antieke klok kan worden verankerd en tegen snelkraak beschermd door het vastzetten ervan met bijvoorbeeld een chemisch anker of keilbout. Zo zijn er ook speciale bevestigingen op de markt om schilderijen te verankeren.

Aanhangwagens zijn moeilijk te ontvreemden en aan te koppelen als deze zijn verankerd door middel van het koppelen van de dissel aan een gefixeerde kogel aan het gebouw (denk aan een bouwmarkt)

Winkel of showroom

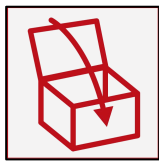
Door boormachines en/of ander elektrisch gereedschap te verankeren aan het schap, is snelkraak na elektronische alarmering moeilijk. Door de boorkop op gefixeerde stiften te plaatsen en/of de machines met kabels te beveiligen, wordt een goed effect verkregen.

Grotere machines als aggregaten, hogedrukreinigers en/of compressoren kunnen met behulp van een zware geplastificeerde kabel worden verankerd aan gefixeerde ankers in de betonnen vloer van de showroom.

Magazijn of opslag

Denk in dit verband ook aan het koppelen van aanhangwagens, grotere verrijd bare opslagen e.d. Elektrotechnische maatregelen zoals het spanningsloos maken van hefdeuren, rolluiken, verlichting, e.d. zijn feitelijk ook meeneembepurende maatregelen die na sluitingstijd effect sorteren.

5.7 C/M 2 niveau prestatie-eis 5 minuten inbraakvertraging



5.7.1 Kisten of kasten

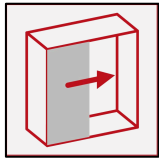
Eigen gebruik Een aannemersbedrijf kan na werktijd zijn elektrisch gereedschap verzamelen in een zelf gemaakte verrijdbare houten kist of grotere kast om inbraak en snelkraak te voorkomen. Let hierbij wel op dat de waardeberging zelf goed wordt gefixeerd, anders is de totale buit in één keer vertrokken. De andere machines in een werkplaats zijn groot en zwaar en dus veel minder attractief, zeker voor een snelkraker. Een dergelijk beleid werkt ook een zekere mate van orde en netheid in de hand en komt het preventiebewustzijn ten goede.

Winkel of showroom

De duurdere elektronica die bijvoorbeeld bij een verkoopadres van bootaccessoires aanwezig is, zoals navigatie - en sonarsystemen, kunnen in een fraaie maar goed afsluitbare houten of stalen kast worden geborgen die deel uitmaakt van de stellingwanden. Door deze kast in de dagsituatie simpelweg open te zetten ontstaat na sluitingstijd een gemakkelijk afsluitbare en effectieve preventieve voorziening tegen snelkraak. Ook tabaksartikelen zouden in een soortgelijke verkoopsituatie kunnen worden uitgesteld.

Magazijn of opslag

Alarm -, audio - en navigatiesystemen zijn bijvoorbeeld bij een grotere autodealer in het magazijn goed geborgen in deugdelijk afsluitbare houten (38 mm hechthout) of stalen kasten. Het hang- en sluitwerk daarvan moet voldoen aan niveau B2 zijn, evenals de bevestiging van bijvoorbeeld de overvalsluiting voor een hangslot. Standaard zwaardere archiefkasten of (tweedehands) grotere safes kunnen veelal dienst doen als opslag van inbraakgevoelige goederen.



5.7.2 Vitrines

Eigen gebruik Een vitrine is in deze situatie eigenlijk geen optie, of het zou zo moeten zijn dat het een verzameling betreft in de woning of op kantoor in een kast met beglazing waarbij gebruik gemaakt wordt van gelaagd glas (Swarowski kristal of antiek)

Winkel of showroom

Goederen als zonnebrillen, luxe artikelen, mobiele telefoons, digitale camera's, computerartikelen etc. kunnen worden gepresenteerd binnen een winkel in afgesloten schappen of vitrines (ook tegen diefstal overdag) Door gebruik te maken van lexan en/of gelaagde beglazing (norm NEN-EN 356) in een deugdelijk kader, met goed sluitwerk kan een beveiligde vitrine worden gerealiseerd. Veelal is het een eigen fabrikaat of zal het vernuft van een vitrinebouwer hierbij doorslaggevend zijn.

Magazijn of opslag

Niet van toepassing.



5.7.2 Hekwerken

Eigen gebruik Een cafébedrijf met audio-installatie en een flinke Cd-opslag achter de bar kan dit attractieve geheel eenvoudig tegen snelkraak beschermen door hiervoor na sluitingstijd consequent een raster of hekwerk te plaatsen en af te sluiten. Apparatuur met Cd's als inhoud en digitale PC-opslag van muziek moet niet worden onderschat qua

attractiviteit en vervangingskosten

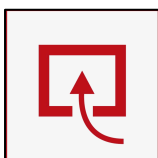
Winkel of showroom

Een inpendig rolluik, rol- of schaarhek (of soms zelfs bouwhek) kan in een hoek van een winkel dienst doen om een compartiment te vormen, waarachter na sluitingstijd de attractieve goederen worden gestald. Het is voor een inbreker de moeilijkste situatie om eenmaal in de winkel en tijdens een elektronisch alarm, een poging te ondernemen om dit hekwerk te slopen. De visuele drempel zal in dit geval ook al in de dagsituatie helpen voorkomen dat een inbreker zijn plannen voor inbraak voorbereidt. Denk in dit verband bijvoorbeeld aan leren motorkleding en accessoires in een motorshowroom en verkoopruimte.

Magazijn of opslag

Een schappengedeelte voor de opslag van attractieve materialen in een magazijn is tegen snelkraak beschermd door de gang - of looppaden te blokkeren met een inpendig hekwerk. Een goede afsluitmogelijkheid en een hek van afdoende hoogte en sterkte zijn dan essentieel. Een hekwerk tussen expeditie en magazijn doet in dit verband ook dienst om te voorkomen dat 'Jan en alleman' een kijkje in de keuken kunnen nemen! Als aandachtspunt geldt dat rekening moet worden gehouden met vluchtwegen

5.8 C/M 3 Niveau prestatie-eis 10 minuten inbraakvertraging



5.8.1 Compartimenten

Eigen gebruik Als voorbeeld kunnen laptops binnen afgesloten gebied worden geborgen in deugdelijk (en dus vaak met extra sloten) afgesloten inpendige ruimten. Een compartiment als dit is binnen het bedrijf vaak een ruimte waarin ook de server, een datasafe, aanwezige duurdere gebruikersgoederen (bijvoorbeeld laserapparatuur) of documenten kunnen worden geborgen of geplaatst. Een dergelijk compartiment dient geheel inpendig te zijn gesitueerd, waarbij een aanval in alle gevallen wordt voorafgegaan door een elektronisch alarm met opvolging. Alle 6 zijden (dus óók de boven - en onderzijde) van het compartiment moeten worden afgeschermd door elektronische detectie.

Winkel of showroom

Als voorbeeld kan hier een zonnebrillenstandaard (verrijdbaar?) worden genoemd in een optiekzaak die consequent na winkelsluiting wordt geplaatst binnen een extra afsluitbaar gemaakt gedeelte, zoals een inpandig kantoor of misschien zelfs een toiletruimte. Mobiele telefoons zijn als voorbeeld na winkelsluiting goed geborgen in een, binnen de winkel of showroom gerealiseerd, compartiment (onder de toonbank, in een tweedehands safe of in een versterkte kast). Een dergelijk compartiment is te realiseren uit hout en/of staal met zwaar sluitwerk.

Magazijn of opslag

Attractieve goederen kunnen worden opgeslagen en/of geplaatst in een standaard of speciaal te realiseren compartiment uit vlechtwerkstaal, hout, baksteen, strekmetaal etc. Zwaar sluitwerk en een sabotagevrije elektronische detectie rondom zijn noodzakelijk. Alle aanvalszijden moeten goed onder de loep worden genomen, waarbij het essentieel is dat een aanval op het compartiment altijd eerst wordt voorafgegaan door elektronische alarmering. De braaktijd en dus de zwaarte van het compartiment, worden afhankelijk gesteld van de waarde van de op te bergen goederen. Met het oog op de alarmopvolging, die vandaag de dag gemakkelijk kan oplopen tot meer dan 15 minuten, zou de ondergrens op deze tijd moeten liggen, oplopend tot meer dan een uur. Standaard oplossingen met keurmerk zijn momenteel in de markt verkrijgbaar. Dit stalen compartiment wordt samengesteld uit modules en segmenten.

Opmerking bij 5.8.1; indeling in niveaus voor compartimenten

In de tabel van de beveiligingsklasse voor bedrijven wordt de vereiste compartimentering aangeduid met C1, C2 of C3. Bij C1 gaat het om een safe of inbraakwerende kast die geschikt is voor de op te bergen waarde. Een compartiment op niveau C1 is een inpandige ruimte waarvan de deur voldoet aan B1 en de vloer, wanden en plafond een gelijkwaardige weerstand bieden. (prestatie-eis 3 minuten inbraakvertraging)

C2 en C3 hebben betrekking op zwaardere bouwkundige compartimenten.

Voor de verschillende compartimenten worden de navolgende eisen gehanteerd.

Bij het inrichten of bouwen van een compartiment kan het gaan om één enkele ruimte of kast, maar ook om een samenstel van ruimten die samen één compartiment vormen.

Bij het inrichten of bouwen gelden de volgende eisen:

Alle bouwkundige afscheidende constructies van het compartiment dienen voldoende fysieke sterkte te bezitten om de vereiste inbraakvertragende werking op te leveren. Dit wil zeggen dat er niet alleen eisen worden gesteld aan de wanden van het compartiment, maar ook aan de andere - mogelijke - aanvalszijden voor inbrekers. Dit betreft dus de vloer, het plafond of het dak van het compartiment, voor zover bereikbaar voor inbrekers.

Wanden: de inbraakwerendheid van de wanden van een compartiment (of vloer, plafond of dak) worden niet alleen bepaald door de dikte of het soort materiaal waaruit deze zijn geconstrueerd. Van belang zijn ook factoren als de verankering of de aanwezigheid van openingen.

De wanden van een C2 of C3 compartiment dienen te bestaan uit gewapend beton of uit metselwerk. Het metselwerk kan worden opgetrokken in baksteen, kalkzandsteen of betonblokken. Lichte blokken of stenen, zoals cellenbeton, lichtbeton, porisosteent e.d., zijn eveneens toepasbaar, mits een dikte wordt aangehouden die twee maal zo groot is als de hierna genoemde waarden.

De dikte van wanden van beton of metselwerk dient ten minste te bedragen voor **C2: 100 mm** en voor **C3: 200 mm**. Indien de hoogte van de wanden meer dan 3 meter bedraagt, dienen de genoemde dikten te worden verdubbeld. Uiteraard kunnen ook wanden worden toegepast die van andere materialen zijn geconstrueerd, mits daarmee een gelijkwaardige inbraakwerendheid wordt verkregen.

De wanden dienen afdoende aan de omliggende constructies te worden verankerd, waarbij de onderlinge afstand tussen de verankeringen niet meer dient te bedragen dan 500 mm.

De wanden dienen te worden opgetrokken tot - en goed aan te sluiten tegen - de bovenliggende vloer- of dakconstructie. In ruimten met systeemplafonds betekent het voorgaande dat de wanden dienen door te lopen tot boven het systeem plafond en aan te sluiten aan de bovenliggende vloer- of dakconstructie. In de wanden dienen bij voorkeur geen ramen aanwezig te zijn. Als er ramen aanwezig zijn dienen ze voorzien te zijn van inbraakwerende beglazing dan wel glasafscherming.

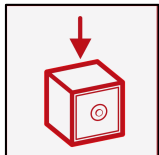
Deuren: deuren in wanden van een **C2** compartiment dienen te voldoen aan de norm NEN 5096 weerstandsklasse 3 (prestaties is 5 minuten) of daaraan gelijkwaardig te zijn. Eventueel aanwezig glas in dergelijke deuren dient vervangen te worden door inbraakwerende beglazing dan wel voorzien van glasafscherming.

Deuren in wanden van een **C3** compartiment dienen minimaal te voldoen aan de norm NEN 5096 weerstandsklasse 4 (prestaties is 10 minuten) of daaraan gelijkwaardig waarbij geen glas bezetting aanwezig dient te zijn. In het PVE kunnen nader gespecificeerde - en op het desbetreffende risico afgestemde - eisen worden gesteld.

Vloer, plafond of dak: de vloer en het plafond of dak maken eveneens onderdeel uit van het compartiment. Voor zover deze afscheidende constructies aan de buitenzijde van het compartiment voor inbrekers bereikbaar zijn, betekent het voorgaande dat ze voldoende inbraakwerend moeten zijn. Indien het mogelijk is om met gebruik van handgereedschap, zoals plaatschaar, decoupeerzaag e.d., een opening te maken waardoor het compartiment betreden kan worden. Bij constructies, zoals een houten vloer of een dak van geprofileerde staalplaten, zullen daarom aanvullende maatregelen getroffen moeten worden. Dit heeft niet alleen betrekking op de elektronische bewaking, maar ook op het aanbrengen van een extra fysieke barrière aan de binnenzijde, bijvoorbeeld in de vorm van een doeltreffende beplating met staalplaat of strekmetaal.

Altijd inbraaksignaleringsysteem

Een compartiment is bestemd voor het opbergen van goederen of zaken die voor inbrekers zeer attractief zijn. De beveiligingstheorie is er daarom opgericht om een inbraak in het gebouw te detecteren nog vóór het compartiment wordt bereikt of aangevallen. Het betekent dat een compartiment altijd moet worden gecombineerd met een inbraaksignaleringsysteem in het gebied buiten het compartiment. Hierbij moet de beveiliging zich uitstrekken tot alle aanvalszijden van het compartiment (dus ook vloer en plafond of dak) Als door het volume van een C2 of C3 compartiment de kans bestaat op insluiting is ruimtelijke detectie ook IN het compartiment verplicht.



5.8.2 Kluizen en safes

Eigen gebruik Om diefstal, en met name snelkraak, te voorkomen, kunnen kleine attractieve goederen in elke situatie worden opgeborgen in een safe of kluis. Essentieel is daarbij dat ook de safe zelf wordt verankerd! Het komt niet zelden voor dat de gehele voorziening verdwijnt; de kluis of safe vormt een wel heel attractief goed op zichzelf... Het spreekt vaak tot de verbeelding van de potentiële crimineel dat het hier een aanzienlijk bedrag aan geld betreft. Ook wanneer dit niet het geval zou zijn en zelfs wanneer dat op de safe zou staan, zal een safe vrijwel altijd boven aan zijn 'verlanglijstje' staan. Het buiten het gezichtsveld plaatsen en/of betimmeren ervan is daarom aan te bevelen.

Winkel of showroom

Bijvoorbeeld een winkel in mobiele telefonie zou als display gebruik kunnen maken van een grotere tweedehands safe, desgewenst gespoten in de bedrijfskleuren. Na sluiting gesloten betreft het vervolgens een prima compartiment. Standaard safes en kluiskasten zijn verkrijgbaar als sigarettenopslag en verkoopkasten.

Magazijn of opslag

Luxe rookwaren en aanverwante artikelen van gerenommeerde merken kunnen binnen een groter magazijn worden opgeborgen in grotere safes. Ook soms aanwezige bouwkundige kluizen kunnen als geen ander dienst doen als goed compartiment voor de berging van hoogwaardige goederen als bijvoorbeeld horloges, laptops, computeronderdelen, software et cetera.

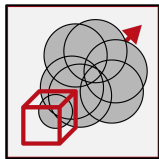
Opmerking bij 5.8.2; dekkingsindicatie

Safe: waardeberging met bescherming tegen inbraak, met een intern grond vlak van < 2m² en
Kluis: waardeberging met bescherming tegen inbraak, met een intern grond vlak van > 2m² die
volgens de inschaling van de Vereniging Geld- en Waardeberging (VGW) geschikt is voor de op te bergen
waarde. Van toepassing is: dekkingsindicatie Weerstandsklasse volgens NEN-EN 14 450 en de
inbraakwering volgens NEN-EN 1143-1

Voor de berging van waardepapieren en digitale datadragers is de NEN-EN 1047-1 van toepassing.

Vrijstaande inbraakwerende kasten en safes die lichter zijn dan 1.000 kg vereisen een sterke
verankering, zie voor de eisen daaraan het document van Vereniging Geld- en Waardeberging.

Voor safes en kluisen die zich binnen het ruimtelijk beveiligd gebied bevinden kan de dekkingsindicatie
worden verdubbeld. Bij een safe of kluis geplaatst in een C2 of C3 compartiment kan de
dekkingsindicatie worden verdrievoudigd (schillentechniek)



5.8.3 Mistgeneratoren

Eigen gebruik Een kostbare particuliere inboedel, met daarin fraaie stukken, of een
gelijke inventaris van een kantoor kunnen goed tegen snelkraak worden beschermd
door middel van mist. Vooral wanneer de beveiliging van de bouwkundige schil
geen uitkomst biedt en/of traliewerken om esthetische redenen niet toelaatbaar zijn.

Een elektronische alarmering activeert de mistuitstoot, die tot soms wel 30 kubieke meter per seconde
kan bedragen.

Winkel of showroom

Een winkel met bijvoorbeeld parfumerie, telefonie en/of ander zeer attractief kleingoed, kan met
mistgeneratoren worden beveiligd. Een duidelijke zichtbare en fysieke drempel van rolluik en/of
hekwerk ontbreekt hier, wat als een nadeel kan worden uitgelegd. De effectiviteit van een beveiliging
met mistgeneratoren is echter groot.

Magazijn of opslag

Een apart gedeelte van een magazijn waar bijvoorbeeld de gehele voorraad elektrisch gereedschap
staat opgeslagen, kan na elektronische detectie binnen de kortste keren in de mist worden gezet. De
elektronische schakeling kan zo zijn opgebouwd dat pas een mistuitstoot volgt wanneer er daadwerkelijk
wordt ingebroken en het detectieveld een toenadering van dit gedeelte van het magazijn 'ziet'.

Duidelijk is dat het projecteren en toepassen van mistgeneratoren met veel zorg en vakkennis moet
plaatsvinden. Met name omdat mist, bij de alarmopvolgers, geen verwarring mag geven met rook
(brand) Zie hiervoor tevens het document D01/026 oktober 2001 versie 2: Mistgeneratoren

6. Alarmering

6.1 Voorgeschiedenis:

In het geval dat een inbraaksignaleringsysteem melding maakt van een onveilige situatie dient hiervan
melding te worden gemaakt bij een Particuliere Alarmcentrale (PAC), van waaruit actie, richting onder
meer de politie, kan worden ondernomen.

Aangezien criminelen graag in de anonimiteit blijven proberen zij op tal van manieren te voorkomen
dat zij ontdekt worden. Een van deze manieren is het saboteren van de alarmtransmissiesysteem
tussen het bewaakte object en de PAC. Deze sabotage kan op een aantal punten in het gehele
transmissietraject. Hierdoor moeten binnen het object een aantal maatregelen genomen worden ten
aanzien van de afscherming van de transmissieleiding(en) zodat een mechanische barrière wordt
opgebouwd die voldoende oponthoud biedt dat bij een eventuele sabotage poging, dan wel
inbraakpoging de melding hiervan altijd bij de PAC wordt gesignaleerd.

Daarnaast dient, zeker bij de hogere risico's, rekening te worden gehouden met het saboteren van de
transmissiesysteem buiten het object. Om genoemde zaken te bewerkstelligen zijn functionele eisen
opgesteld ten aanzien van twee transmissietrajecten, te weten het AL1 en het AL2 traject. De eisen
voor deze trajecten zijn afkomstig uit de Nederlandse/Europese norm NEN-EN-50136-1-1.

Het AL1 traject is met name van toepassing op de lage risicosegmenten (woonhuizen, eenvoudige winkels en bedrijven) en omvat in principe alle gekozen verbindingen zoals de toepassing van een Automatisch Telefoonkiezer (ATK), GSM-telefoon etc. Ook combinaties van dergelijke systemen zijn mogelijk.

Het AL2 traject daarentegen is afgestemd op de hoge risicosegmenten en omvat een continu bewaakte transmissieweg.

6.2 Europese normen

De functionele eisen zijn afgeleid van de Europese en ook in Nederland gehanteerde normen, te weten: NEN-EN 50136-1-1 'Alarm systems - Alarm transmission systems and Equipment

Part 1-1: General requirements for alarm transmission systems'

In deze norm staan de algemene, functionele, eisen ten aanzien van transmissiesystemen en de voor deze systemen toe te passen apparatuur.

NEN-EN 50136-1-2 'Alarm systems - Alarm transmission systems and Equipment

Part 1-2 : Requirements for systems using dedicated alarm paths'

In deze norm staan de eisen vermeld waar met name transmissiesystemen voor het AL2 traject aan dienen te voldoen.

NEN-EN 50136-1-2 'Alarm systems - Alarm transmission systems and equipment.

Part 1-3 : Requirements for systems with digital communicators using the public switched telephone network'.

In deze norm staan eisen vermeld waaraan met name transmissiesystemen voor het AL1 en AL2 traject dienen te voldoen.

NEN-EN 50136-2-1 'Alarm systems - Alarm transmission systems and Equipment

Part 2-1 : General requirements for alarm transmission equipment'.

In deze norm staan de algemene eisen ten aanzien van toe te passen apparatuur binnen transmissietrajecten.

NEN-EN 50136-2-2 'Alarm systems - Alarm transmission systems and equipment.

Part 2-2: Requirements for equipment used in systems using dedicated alarm path'.

In deze norm staan eisen vermeld waaraan apparatuur voor met name de toepassing in het AL2 traject dient te voldoen.

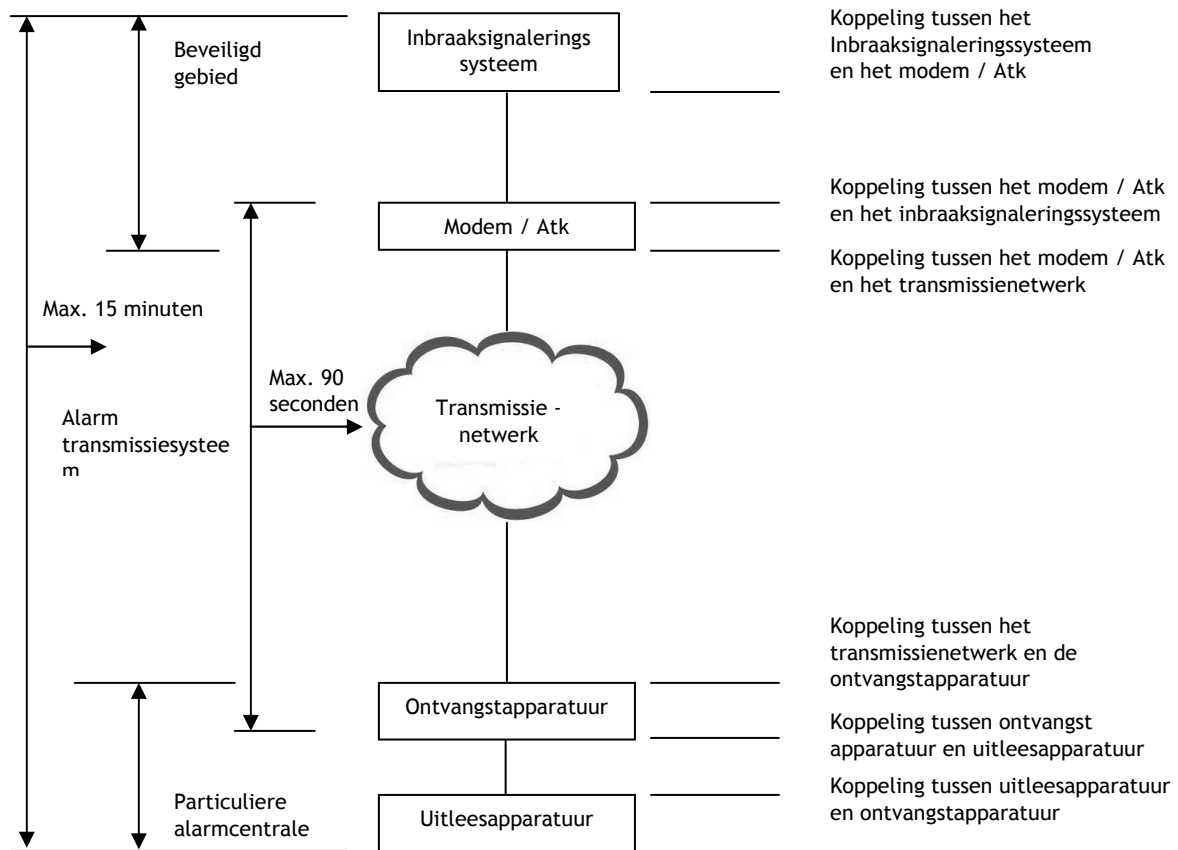
NEN-EN 50136-2-3 'Alarm systems - Alarm transmission systems and equipment

Part 2-3 : Requirements for equipment used in systems with digital communicators using the public switched telephone network'.

In deze norm staan eisen vermeld ten aanzien van apparatuur geschikt voor het AL1 en AL2 traject.

De genoemde normen geven een goed inzicht in de functionele en prestatie-eisen waaraan zowel het transmissiesysteem als de toe te passen apparatuur binnen de genoemde systemen dienen te voldoen.

Communicatieapparatuur die wordt toegepast, dient te worden getest volgens de in de normen vermelde eisen ten aanzien van deze apparatuur. Tevens geven de normen duidelijk aan welke transmissietrajecten gecontroleerd dienen te worden in de aangegeven testtijden T1 tot en met T5 (zie schema)



6.3 Kenmerken

De functionele eisen zijn samengesteld uit de kenmerken zoals die staan omschreven in de NEN-EN 50136:

Deze kenmerken zijn:

Voor AL1 geldt: D2, M2, T2, A2

Voor AL2 geldt: D3, M3, T5, A3, dan wel netwerksigalering met een responstijd van 20 sec op de locatie van de PAC, alsmede ter plekke van het risicoadres.

In geval van netwerksigalering wordt tussen het bewaakte object en de PAC een 'staande verbinding' opgebouwd (end to end) Deze verbinding wordt continu in stand gehouden, zij het dat er over deze verbinding geen signalen worden verstuurd en er zodoende gesproken wordt over een 'virtuele verbinding'. Gebeurt er iets met deze verbinding dan moet hiervan binnen 20 seconden melding gemaakt worden bij de PAC. Ter controle van de in de transmissieweg opgenomen apparatuur, dient om de 15 minuten een controlebericht (end to end) te worden verzonden. Mocht dit bericht niet door de PAC worden ontvangen, dan moet de PAC hiervan binnen 30 seconden worden bericht.

Voor de genoemde coderingen gelden de hieronder vermelde waarden.

Transmissietijd

Rekenkundig gemiddelde van de gehele datatransmissie: D2 = 60 sec
D3 = 20 sec

Bovenste 95% van de gehele datatransmissie: D2 = 80 sec
D3 = 30 sec

Maximale transmissie-tijd

Maximale acceptabele transmissietijd:
M2 = 120 sec
M3 = 60 sec

Testmelding

Maximale periode: T2 = 25 uur
T5 = 90 sec

In afwijking op de norm geldt permanente netwerksignalering met end to end controle op gebruikte transmissieapparatuur van 15 minuten.

Beschikbaarheid

Algemene beschikbaarheid van A2 = 99,3 %
het systeem over 12 maanden: A3 = 99,5 %
Maandelijkse beschikbaarheid: A2 = 91,0 %
A3 = 95,0 %

6.4 Aanvullende bepalingen

Voor beide transmissiesystemen dienen maatregelen getroffen te worden ter voorkoming van het nabootsen van het transmissiesysteem in het beveiligde gebouw.

Bij AL1 dient dit te geschieden door: het toevoegen van een identiteit of een adres aan alle uitgezonden signalen over het alarmtransmissiepad.

S: substitutie beveiliging c.f. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.5.1: S1 = toevoeging van een identiteit of adres aan elk via het alarmtransmissietraject verzonden bericht.

Bij AL2 dient dit te geschieden door: encryptie van een identiteit of een adres van alle uitgezonden signalen over het alarmtransmissiepad,

S: substitutie beveiliging c.f. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.5.1: S2 = toevoeging van encryptie van identiteit, of authenticatie door een verschillende en niet openbare code voor iedere aangesloten alarmoverdrager, of een door de fabrikant gespecificeerde methode.

of:

autorisatie bij het in het beveiligde object aanwezige transmissiesysteem door middel van verschillende niet te decoderen codes voor ieder aanwezig transmissiesysteem,

of:

een andere door de fabrikant gespecificeerde methode.

Ten aanzien van de informatiebeveiliging:

c.f. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.5.2

I0 = geen maatregelen

I2 = maatregelen ter voorkoming van ongeautoriseerde wijziging van verzonden informatie

I3 = maatregelen ter voorkoming van ongeautoriseerde wijziging en lezen van verzonden informatie

Samengevat:

De Europese normen NEN-EN 50131-1 en NEN-EN 50136-1-1 kennen t.o.v. de Nederlandse

benadering een afwijkende systematiek en afwijkende prestatie-eisen. Voor wat betreft

alarmtransmissiesystemen worden in de Europese normen 6 klassen gehanteerd, te weten ATS1,

ATS2, ATS3, ATS4, ATS5 en ATS6.

Het alarmtransmissietraject AL1 komt overeen met ATS3 in de NEN-EN 50131

(tabel 11 Alarm transmission system performance criteria)

Het alarmtransmissietraject AL2 komt overeen met ATS5 in de NEN-EN 50131

(tabel 11 Alarm transmission system performance criteria) met als aanvulling dat voor de Reporting time classification (testmelding) T5 van toepassing is (90 seconden) i.p.v. T4 (180 seconden)

Het toegepaste transmissiesysteem is afhankelijk van de infrastructuur van de PAC.

De PAC dient dan ook een verklaring af te geven dat de structuur aanwezig is voor het gekozen alarmtransmissiesysteem.

6.4.1 Alarm over IP

Onderstaande tabellen 1 en 2 zijn van toepassing bij alarmtransmissie over IP netwerken

TABEL 1

	Primaire verbinding	T rapportagetijd	Secundaire verbinding	T rapportagetijd standby	T rapportagetijd In bedrijf *	D	M	S	I	beschikbaarheid	
										12 maanden	per maand
AL1	IP ook internet	T2 (25 uur)	Back-up	T2 (25 uur)	T2 (25 uur)	D2	M2	S1	I2	99,3 %	91,0 %
AL2	Besloten IP VPN	T4 (180 sec)	Back-up	T2 (25 uur)	T3 (300 min)	D3	M3	S2	I3	99,5 %	95,0 %

* = indien primaire verbinding niet beschikbaar

Toelichting:

T = rapportagetijd c.f. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.3.4 - tabel 3

In de praktijk wordt invulling gegeven aan de classificatie rapportagetijd middels testmeldingen (functionaliteit op laag 7 OSI model)

Voor wat betreft de rapportagetijd niveau AL2 is gekozen voor het niveau van ATS 5 NEN-EN 50131-1, dit betekent T4 (180sec) i.p.v. T5 (90 sec)

D = gemiddelde transmissietijd conform. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.3.2 - tabel 1

D2 = gemiddelde transmissietijd: 60 sec. en 95% van alle transmissies: 80 sec.

D3 = gemiddelde transmissietijd: 20 sec. en 95% van alle transmissies: 30 sec.

M = maximale transmissietijd conform. NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.3.2 - tabel 2

M2 = 120 sec.

M3 = 60 sec.

S = substitutie beveiliging conform NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.5.1

S0 = geen maatregelen.

S1 = toevoeging van een identiteit of adres aan elk via het alarmtransmissietraject verzonden bericht.

S2 = toevoeging van encryptie van identiteit, of authenticatie door een verschillende en niet openbare code voor iedere aangesloten alarmoverdrager, of een door de fabrikant gespecificeerde methode.

I = informatie beveiliging conform NEN-EN 50131-1:2006 par. 8.6 - tabel 10 en 11 en NEN-EN 50136-1-1 par. 6.5.2

I0 = geen maatregelen.

I2 = maatregelen ter voorkoming van ongeautoriseerde wijziging van verzonden informatie.

I3 = maatregelen ter voorkoming van ongeautoriseerde wijziging en lezen van verzonden informatie.

Beschikbaarheid per 12 maanden en per maand van het totale alarmtransmissiesysteem conform NEN-EN 50136-1-1 par. 6.4.5 - tabel 4

Rapportagetijd:

In de praktijk wordt de invulling gegeven aan de classificatie Rapportagetijd middels testmeldingen.

6.4.2 Back-up verbinding (EN 50136-1-1 artikel 6.3.4)

Een aanvullend benodigde communicatieroute voor alarmoverdracht in het geval dat de primaire communicatieroute niet aan de prestatie-eisen kan voldoen. Gedurende de periode (standby) dat een aanvullende communicatieroute (back-up) niet in gebruik is als primaire communicatieroute, mag de rapportagetijd van de aanvullende communicatieroute verschillen t.o.v. de primaire route.

6.4.3 Prestatieniveau AL1, AL2

Het prestatieniveau van het totale alarmtransmissiesysteem wordt bepaald door het component van het alarmtransmissiesysteem met het laagst (haalbare / ingestelde) prestatieniveau. Voorbeeld: indien door toepassing van een conversieapparaat het prestatieniveau vanaf het conversieapparaat t/m de ontvangstapparatuur conform AL2 is ingesteld en de toegepaste alarmoverdrager staat op AL1 ingesteld dan zal het prestatieniveau van de het totale alarmtransmissiesysteem uitkomen op AL1.

6.4.4 Internet

Internet is een IP netwerk en is open en toegankelijk voor iedereen met de daaraan verbonden voor- en nadelen. Internet voldoet niet aan de toepasselijke prestatie-eisen en de performance van iedere afzonderlijke aansluiting kan sterk verschillen t.o.v. overige aansluitingen. Zonder aanvullende maatregelen is Internet niet geschikt als drager voor alarmtransmissie. Deze maatregelen kunnen, afhankelijk van het risico op de locatie, bestaan uit één van de eerder genoemde back-up mogelijkheden voor alarmdoormelding.

6.4.5 Besloten netwerk/verbinding

Een netwerk of alarmtransmissieverbinding dat/die zodanig is ingericht dat de alarmcommunicatie niet beïnvloed kan worden door andere applicaties en/of diensten die ook gebruik maken van hetzelfde netwerk en/of netwerkverbinding. Deze eis kan ingevuld worden door het gebruik van bijvoorbeeld Quality-of-Service of, beter nog, een 2e VC. IPSec voldoet hier niet aan, want op één en dezelfde lijn zonder aanvullende maatregelen kan IPSec nog steeds beïnvloed worden door andere applicaties.

6.4.6 VPN:

Traditionele IP-netwerken zoals het Internet schieten doorgaans tekort op het vlak van beveiliging en reservering van een dedicated bandbreedte (bijvoorbeeld in de vorm van Quality of Service (QoS), een 2e ATM Virtueel Circuit of een 2e VLAN om gebruikt te kunnen worden voor hoogwaardige telecommunicatie wat voor alarmverkeer een vereiste is. Een Virtual Private Network (IP-VPN) verbindt lokale bedrijfsnetwerken met elkaar tot één besloten communicatienetwerk, van en onder beheer van de netwerkprovider, zonder tussenkomst van het Internet. Het gaat daarbij niet alleen om alarm, spraak en dataverkeer, maar ook om e-mail en het gebruik van belangrijke centrale systemen. Wanneer de provider de benodigde routers beheert, is men in staat om over het gehele transport traject controle uit te voeren over de dienstverlening. Quality of Service (QoS), een 2e ATM Virtueel Circuit of een 2e VLAN maakt het mogelijk om bedrijfskritische applicaties (zoals alarmcommunicatie) voorrang te geven boven ander (niet-bedrijfskritisch) netwerkverkeer. Beheerde of gemanagede VPN aansluitingen zijn doorgaans duurder dan de traditionele (Internet) aansluitingen.

6.4.7 Voorkeurschakeling

Het alarmtransmissiesysteem dient zodanig te worden ingericht dat de alarmcommunicatie altijd voorrang heeft op de overige diensten/applicaties die gebruik maken van dezelfde netwerkaansluiting(en). Door gebruik te maken van bepaalde back-uproutes voor alarmcommunicatie kan deze eis komen te vervallen tenzij de betreffende back-uproute zelf voorzien moet worden van een dergelijke voorkeurschakeling.

Zie voor de volledige informatie de vigerende versie “Advies Praktijkrichtlijn Alarmtransmissie over IP-netwerken” van het VvBO

Tabel 2

Alarmtransmissie over analoge en ISDN verbindingen						
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 3*	Klasse 4	Klasse 4*
Woningen	AL0	AL1	AL1	n.v.t.	AL2	AL2
Bedrijven	AL1	AL1	AL1	AL2	AL2	AL3
Alarmtransmissie over IP netwerken						
Risicoklasse	Klasse 1	Klasse 2	Klasse 3	Klasse 3*	Klasse 4	Klasse 4*
Woningen	AL0	Internet + back-up *	Internet + back-up *	n.v.t.	besloten netwerk + back-up	n.v.t.
Bedrijven	Internet + back-up *	Internet + back-up *	Internet + back-up	besloten netwerk + back-up	besloten netwerk + back-up	besloten netwerk + back-up

* In afwijking van het advies Praktijkrichtlijn alarmtransmissie over IP netwerken:
Bij risicoklasse 2 en 3 voor woningen is het ontbreken van een back-up traject toegestaan.
Bij risicoklasse 1 en 2 voor bedrijven is het ontbreken van een back-up traject toegestaan.
In die situaties dienen alle stroomverbruikende componenten die tussen alarmoverdrager en het ISRA punt zijn geplaatst en onderdeel zijn van het alarmtransmissiesysteem voorzien te zijn van een noodstroomvoorziening die toereikend is om de alarmtransmissie mogelijk te maken. Dit kan o.a. worden gerealiseerd door gebruik te maken van de noodstroomvoorziening van de CCS. Houdt hierbij wel rekening met de accu capaciteit voor het volledige systeem. Deze afwijking is niet van toepassing op overvalmeldingen middels Alarmtransmissie over IP netwerken.

Uitval van de primaire verbinding dient te worden doorgemeld via de back-up verbinding naar de PAC. Uitval van de back-up verbinding dient te worden doorgemeld via de primaire verbinding naar de PAC. De back-up verbinding dient bij gebruik van een analoge lijn te zijn uitgevoerd met kiestoondetectie. Indien een back-up route (analoog of ISDN) gebruik maakt van een shared line dan dienen aanvullende maatregelen te worden getroffen om de back-up alarmcommunicatie over deze shared line te borgen, dit kan middels een voorkeurschakeling onder controle van het alarmsysteem of overdrager of door toepassing van een beveiligde splitter welke wordt gevoed vanuit het alarmsysteem en rapporteert aan het alarmsysteem in de situatie dat er sprake is van het aanspreken van de beveiligingsfunctie m.b.t. de verstoring op de shared line. Opvolging door de PAC bij deze uitvalmeldingen dienen te worden opgevolgd conform daarover schriftelijk vastgelegde afspraken.

6.5 AL0 traject

Alleen van toepassing in combinatie met een alarminstallatie niveau Ed.

Alarmering:

Bij een alarmsituatie dient na maximaal 60 seconden een alarm te worden gegenereerd.

Alarmering vindt plaats door middel van ten minste één van de volgende alarmeringsmogelijkheden:

1. akoestische alarmering binnen
2. akoestische alarmering buiten
3. optische alarmering
4. melding naar een (mobiele) telefoon

ISDN

Bij ISDN - aansluitingen vervalt bij niveau Ed de eis een voorkeurschakeling toe te passen voor de telefoonkiezer (art 4.3.2 in document 002080) en een nadere omschrijving van deze alarmeringsmogelijkheden vindt u in document 002080 juli 2000 versie 2: Installatievoorschriften voor Alarmapparatuur.

6.6 AL 1 traject

Bij een alarmsituatie dient na maximaal 60 seconden binnen het gebouw een akoestisch alarm te worden gegenereerd, alsmede een optische alarmering die goed zichtbaar is vanaf de openbare weg. Akoestische alarmgevers binnen, moeten zodanig zijn geplaatst dat binnen het beveiligde gebied het geluid ervan duidelijk is waar te nemen. Met duidelijk wordt bedoeld een minimale geluidsterkte van 60 dB(A) gemeten ter plaatse waar zich de attractieve goederen normaliter bevinden.

Dit is ook van toepassing op een sabotagealarm als het alarmsysteem in de in-fase staat. Bij sabotage van een luid-alarmgever dient minimaal een tweede alarmgever te blijven functioneren. (tenzij alarmgevers gelijktijdig worden gesaboteerd) het voorgaande is ook van toepassing bij deel-inschakeling van het alarmsysteem. In de praktijk betekent dit dat er minimaal 2 luid-alarmgevers moeten zijn geïnstalleerd waarvan deze ieder op een apart gezeekerde sirene-uitgang van de CCS of uitbreidings-unit moeten zijn aangesloten. Het kortsluiten of onderbreken van een kabel naar een alarmgever mag dus niet leiden tot uitval van de tweede alarmgever.

Als een beveiligd object bestaat uit meerdere gebouwen is deze eis voor ieder afzonderlijk bouwdeel van toepassing. De eis is niet van toepassing in woningen in risicoklasse 1, 2 en 3, en bedrijven in klasse 1. Hier kan worden volstaan met 1 luid-alarmgever.

Dit in de geest van de praktijkrichtlijn NPR-CLC/TS 50131-7, functionaliteit alarmsystemen NPR-CLC 50131-3.

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding een systeem te worden toegepast van het AL1 traject. De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten particuliere alarmcentrale (PAC) Minimaal één keer per 24 uur dient een controlemelding plaats te vinden.

Noot 6.6 Voor de eisen aan het AL1 traject zie artikel 6.3 en 6.4 (en bij alarm over IP artikel 6.4.1).

6.7 AL 2 traject

Zie voor de eisen voor de akoestische - en optische alarmgevers bij AL1:

Met betrekking tot de alarmering dient voor het versturen van de alarmmelding een systeem te worden toegepast van het niveau AL2. De alarmoverdracht dient te geschieden naar een door het ministerie van Justitie toegelaten particuliere alarmcentrale (PAC)

Noot 6.7 Voor de eisen aan het AL2 niveau zie artikel 6.2, 6.3 en 6.4 (en bij alarm over IP artikel 6.4.1).

6.8 AL 3 traject

Ook een AL2 verbinding kan uitvallen of worden gesaboteerd. In dat geval is het belangrijk dat er communicatie naar de PAC kan plaatsvinden waarmee wordt beoogd dat gedetailleerde informatie over plaats van de alarmering (zone benaming) e.d. beschikbaar is voor de alarmopvolger(s). Bij uitval van de AL2 verbinding dient er een back-up alarmtransmissietraject beschikbaar te zijn via een andere transmissieweg (kabel, mobiel, tweede fysieke aansluiting, e.d.) het traject van deze back-up moet voldoen aan de eisen voor AL1. Uitval van de primaire AL2 verbinding moet binnen 180 seconden te worden doorgemeld via de back-up verbinding naar de PAC. Uitval van de back-up verbinding dient te worden doorgemeld via de primaire verbinding naar de PAC. Opvolging door de PAC bij deze uitvalmeldingen dienen te worden opgevolgd conform daarover schriftelijk vastgelegde afspraken.

Noot 6.8 Voor de eisen aan het AL1 en AL2 trajecten zie artikel 6.3 en 6.4

6.9 Tips om nodeloos alarm te voorkomen

De meeste meldingen van alarminstallaties zijn nodeloos. In veel gevallen zijn bedieningsfouten daarvan de oorzaak. Nodeloos alarm geeft de politie handenvol werk. Met wat meer aandacht van de gebruiker is het mogelijk om hieraan iets te doen.

6.9.1 Bij aanschaf

- Laat de installatie aanleggen door een gecertificeerd BORG Beveiligingsbedrijf of BORG Alarminstallateur. Deze bedrijven werken volgens de installatievoorschriften voor alarmapparatuur.
- Let op de gebruikersvriendelijkheid: van belang is dat een bedieningsmogelijkheid wordt gebruikt die voor de omgeving, de situatie en de personen die deze moeten bedienen, het meest geschikt is.

6.9.2 Nieuwe alarminstallatie in gebruik nemen

- Stel een oefenperiode in om met de nieuwe installatie te leren omgaan. Maak hierover een afspraak met de installateur en de alarmcentrale. Ga pas daarna op een definitieve aansluiting over.
- Houdt het aantal mensen dat de installatie kan in- en uitschakelen zo klein mogelijk. Zorg dat ze goed geïnstrueerd zijn.

6.9.3 Toch nodeloos alarm?

Waarschuw onmiddellijk de alarmcentrale als u per ongeluk een alarm veroorzaakt. De centrale kan een doormelding aan de alarmopvolger dan wellicht nog voorkomen.

6.9.4 Voorkom nodeloos alarm

- Maak met de alarmcentrale een afspraak over de manier waarop u hen bericht als u een fout maakt bij het in- of uitschakelen.
- Heeft u het telefoonnummer van de alarmcentrale bij de hand?
- Laat de installatie nazien als de oorzaak van een nodeloos alarm niet bekend is. Soms kan een kleine technische verandering herhaling voorkomen.
- Zorg dat iedereen die de installatie in- en uitschakelt ook weet wat er moet gebeuren, als hierbij een alarm wordt veroorzaakt.
- Maak voor het inschakelen altijd een afsluitronde. Overtuig u ervan dat alle ramen en deuren gesloten zijn. En denk aan eventuele huisdieren.
- Geef aan de alarmcentrale voldoende waarschuwadressen op. Controleer regelmatig of deze opgave van personen en hun telefoonnummers nog correct is.

7 Reactie (alarmopvolging)

Alle elektronische maatregelen ten spijt, als de alarmopvolging faalt is het doel niet bereikt.

7.1 Indeling in niveaus

In de tabellen van de beveiligingsklasse voor woningen en bedrijven worden de vereiste procedures aangeduid met R0, R1, R1 of R3.

7.2 R0 niveau

Alleen van toepassing bij een alarminstallatie van niveau Ed voor woningen.

In deze situatie wordt de alarmering door het alarmsysteem gemeld naar een mobiele telefoon (spraak of sms bericht). Voor een adequate alarmopvolging is het belangrijk dat deze mobiele telefoon bereikbaar is. Er is geen garantie of controle of de melding tijdig de alarmopvolger bereikt. Ook kan de melding in een voice-mail terechtkomen. Alarmmeldingen van het niveau Ed mogen ook naar een servicecentrale (niet zijnde een PAC) worden doorgemeld. De alarmopvolging geschiedt door persoonlijke verificatie door de eigenaar of sleutelhouder(s)

7.3 R1 niveau

Reactie alarmopvolging: alarmopvolging door sleutelhouder(s) die door de PAC worden gebeld.

Bij de PAC dienen minimaal 2 sleutelhouders te zijn opgegeven. Bij een alarmmelding, waarbij alarmverificatie met technische middelen ontbreekt of leidt tot een negatieve verificatie, wordt de sleutelhouder gebeld. Het is dus belangrijk dat sleutelhouders bereikbaar zijn (gegevens actueel houden) en in staat om eerst persoonlijk te verifiëren of de alarmmelding niet nodeloos is.

De sleutelhouder dient bij mogelijk vermoeden ter plaatse dat het inbraakalarm door een criminele handeling is veroorzaakt de PAC daarvan op de hoogte te stellen of zelf 112 te bellen. Uitgangspunt is alarmopvolging binnen maximaal 20 minuten.

7.4 R2 niveau

Reactie alarmopvolging: procedure als bij R1 met de aanvulling dat voor de alarmopvolging een contract dient te zijn gesloten met een door het ministerie van Justitie erkend particulier beveiligingsbedrijf, dat onder meer als sleutelhouder kan fungeren.

Sleutelhouder(s) dienen wel bij de PAC te blijven geregistreerd voor terugkoppeling bij calamiteiten. Uitgangspunt is alarmopvolging binnen maximaal 15 minuten.

7.5 R3 niveau

Reactie alarmopvolging: procedure als bij R2 (dus opvolging door een particulier beveiligingsbedrijf) Minimaal dient ook één van de drie technische alarmverificatie mogelijkheden operationeel te zijn.

Uitgangspunt is opvolgingstijd van maximaal 15 minuten door de bewakingsdienst en een prioriteit 1 van de politie. (15 minuten, na technisch alarmverificatie)

Indien niet haalbaar dan dient de vertragingstijd gelijkwaardig verhoogd te worden.

Sleutelhouder(s) dienen wel bij de PAC te blijven geregistreerd voor terugkoppeling bij calamiteiten.

7.6 Alarmverificatie

Op dit moment is het onderwerp alarmverificatie in een ontwikkelingsstadium. Een tekst voor dit onderdeel wordt nader ingevuld. Zie hiervoor het (de) vigerende document(en) op de website van het VvBO

7.7 alarmverificatie methoden

- 7.7.1 inkijken
- 7.7.2 inluisteren
- 7.7.3 dubbele zone
- 7.7.4 persoonlijke verificatie

8 Bijlage 1. Modelformulier Programma van Eisen (PvE)

1: gegevens			
Projectnummer	: conform BRL BORG 2005 versie 2 artikel 6.5		
Datum opmaak	:		
Beveiligingsbedrijf Adres / Plaats Telefoonnummer	: : :		
PvE ingevuld door	: bevoegd persoon conform artikel 6.3.3 BRL BORG 2005 versie 2 : naam:.....		
Aanduiding object	: <input type="checkbox"/> woning <input type="checkbox"/> bedrijf <input type="checkbox"/> winkel / showroom <input type="checkbox"/> magazijn/opslag : <input type="checkbox"/> school lager onderwijs <input type="checkbox"/> school middelbaar en hoger onderwijs.		
Bewoner / eigenaar / beheerder Adres / Plaats Telefoonnummer	: : :		
Eisende partij(en)	: <input type="checkbox"/> bewoner / eigenaar / beheerder : <input type="checkbox"/> verzekeraar : <input type="checkbox"/> anders namelijk:		
<input type="checkbox"/> Woningen	: <input type="checkbox"/> verzekerde waarde attractieve zaken €		
Doel van de beveiliging: <input type="checkbox"/> inbraak en diefstalbev. <input type="checkbox"/> brandbeveiliging <input type="checkbox"/> informatiebeveiliging. <input type="checkbox"/> overvalbeveiliging <input type="checkbox"/> toegangsbeveiliging <input type="checkbox"/>	: <input type="checkbox"/> bedrijven : attractiviteit goederen, bedrijfsuitrusting/inventaris : <input type="checkbox"/> Laag verzekerde waarde €..... : <input type="checkbox"/> Midden verzekerde waarde €..... : <input type="checkbox"/> Hoog verzekerde waarde €		
Geconstateerde risicoklasse:	: conform document D0-375 of D03-376 mei 2007 <input type="checkbox"/> klasse 1 <input type="checkbox"/> klasse 2 <input type="checkbox"/> klasse 3 <input type="checkbox"/> klasse 4		
Gekozen combinatie van Beveiligingsmaatregelen <input type="checkbox"/> Noot: bij onderwijsinstellingen de O, B, C/M en E maatregelen conform de richtlijn.	conform definities document D03-385 mei 2007 : <input type="checkbox"/> O1 <input type="checkbox"/> O2 Organisatorische maatregelen : <input type="checkbox"/> B0 <input type="checkbox"/> B1 <input type="checkbox"/> B2 <input type="checkbox"/> B3 Bouwkundige maatregelen : <input type="checkbox"/> C/M1 <input type="checkbox"/> C/M2 <input type="checkbox"/> C/M3 Meeneembeperkende maatregelen : <input type="checkbox"/> Ed <input type="checkbox"/> E1 <input type="checkbox"/> E2 <input type="checkbox"/> E3 Elektronische maatregelen : <input type="checkbox"/> AL1 <input type="checkbox"/> AL2 <input type="checkbox"/> AL3 Alarmtransmissie : <input type="checkbox"/> R1 <input type="checkbox"/> R2 <input type="checkbox"/> R3 Reactie alarmopvolging : <input type="checkbox"/> video <input type="checkbox"/> audio <input type="checkbox"/> meerdere zones Alarmverificatie : <input type="checkbox"/> persoonlijke verificatie sleutelhouder <input type="checkbox"/> bewakingsdienst		
Onderhoud	: contract voor onderhoud. maal per jaar		
Op te leveren met kwaliteitsdocument:	: <input type="checkbox"/> BORG Beveiligingscertificaat : <input type="checkbox"/> BORG Opleveringsbewijs alarminstallatie : <input type="checkbox"/> BORG Opleveringsbewijs bouwkundige beveiliging : <input type="checkbox"/> anders:		
Maatwerk / afwijkingen:	: Toelichting: in een bijlage <input type="checkbox"/> ja <input type="checkbox"/> n.v.t : projectnummer vermelden.....		
2: autorisatie			
Bewoner / eigenaar / beheerder	naam..... telefoonnummer.....	datum	handtekening
Verzekeraar bij klasse 4 verplichte handtekening	Verzekeraar:..... naam:..... telefoonnummer	datum	handtekening
Beveiligingsbedrijf	naam:..... telefoonnummer	datum	handtekening

