

Terrorisme en extremisme

Welke maatregelen kunnen de bedrijven nemen?



Inhoudstafel

Voorwoord	3
Inleiding	5
DEEL 1	7
Fenomeenanalyse: terrorisme in de bedrijfswereld	
1 Definiëringen van terrorisme	7
2 Verschijningsvormen	9
2.1 Algemeen	9
2.2 Terrorisme ten aanzien van de bedrijfswereld	10
3 Fasen in de organisatie van een terroristisch misdrijf	11
DEEL 2	14
Preventiemanagement	
1 Preventie	15
2 Risicoanalyse door het bedrijf	16
2.1 Dreigingsanalyse	17
2.2 Risicoanalyse	18
3 Het ontwikkelen van een strategie	20
4 Het ontwikkelen van het plan	21
4.1 Business Continuityplan: situering	21
4.2 Business Continuityplan: invulling	22
5 Evaluatie van het plan	23
6 Conclusie	23
DEEL 3	25
Preventieve maatregelen	
1 Organisatorische maatregelen	26
1.1 Sensibiliseringsacties en trainingen voor werknemers	26
1.2 Kwaliteitscontroles op het product	27
1.3 Overzichtelijke bedrijfsinrichting en ordelijke huishouding	27
1.4 In- en uitgangen	27
1.5 Toegangswegen	28
1.6 Zichtbaar optreden in de onderneming	29

1.7 Contact met cliënteel, bezoekers en leveranciers	29
1.8 Sleutelplan en sleutelbeheer	29
1.9 Bommelding	31
1.10 Verdachte zendingen (en verdachte voertuigen)	32
1.11 Andere NBCR-incidenten	34
1.12 Geheime documenten	36
2 (Bouw)technische maatregelen	36
2.1 Deuren	37
2.2 Verlichting	37
3 Elektronische maatregelen	38
3.1 Alarminstallatie	39
3.2 Camerasystemen	39
4 ICT-maatregelen	41
4.1 Algemene preventieve ICT-aanbevelingen	41
4.2 Concrete preventieve ICT-aanbevelingen	42
4.3 Aanbevelingen voor slachtoffers van ICT-criminaliteit	43
5 Personele beveiliging	44
Conclusie	45

Voorwoord

Deze brochure, die een algemeen overzicht tracht te geven betreffende de beveiliging tegen terroristische en extremistische acties in de private sector, is tot stand gekomen door de samenwerking tussen de private (VBO)¹ en de publieke sector, en dit in de schoot van de werkgroep “terrorisme” die opgericht is het raam van een algemeen privaat – publiekoverlegplatform “POB”². Let wel, deze brochure heeft nooit de bedoeling gehad om nieuwe beschermingsmaatregelen te ontwikkelen, doch uitsluitend om bestaande en toegepaste beveiligingsmaatregelen rond terrorisme en extremisme op een overzichtelijke manier samen te bundelen.

Deze werkgroep gaf zich twee doelstellingen: enerzijds het creëren van een communicatiekanaal tussen de beide sectoren in geval van terroristische of extremistische acties, en anderzijds het opstellen van een brochure door de publieke sector ten voordele van de private sector, met name hoe deze laatste zich kan beveiligen tegen mogelijke acties van terroristische of extremistische aard.

De eerste doelstelling werd reeds verwezenlijkt door de creatie van een gezamenlijk “Early Warning System”, zijnde een informatievierkant, zodat er een betere informatiedoorstroming plaatsvindt tussen beide sectoren.

Om het terrorisme in de kiem te smoren kunnen er naast acties ondernomen door de overheid, ook preventieve stappen worden genomen door de private ondernemingen. Bedrijven dienen er immers rekening mee te houden dat terroristen of extremisten met hun acties schade kunnen aanrichten, die verstrekkende gevolgen kunnen hebben van diverse aard. Door een preventief beleid op te stellen, kan een terroristische of extremistische actie eventueel worden voorkomen, of in elk geval zou de mogelijke schade kunnen worden gereduceerd.

De brochure bestaat uit drie delen. Het *eerste* deel omvat een fenomeenanalyse van terrorisme gelinkt aan de bedrijfswereld. Het *tweede* gedeelte omschrijft hoe de principes van het “preventiemanagement” in de onderneming kunnen geïmplementeerd worden en met welke factoren kan rekening worden gehouden opdat een dergelijk “preventiemanagement” effectief kan zijn. Nadat we de dreigings-

¹ VBO = Verbond van Belgische Ondernemingen

² POB = Permanent Overlegplatform Bedrijfsbeveiliging

en risicoanalyse bespreken, gaan we over tot de stappen van een Business Continuityplan, zodat onverwachte situaties overbrugd kunnen worden. Het *derde* en laatste gedeelte beschrijft de preventieve tips, aanbevelingen en raadgevingen zodat de onderneming een succesvol preventief antwoord kan geven op concrete of potentiële terroristische of extremistische dreigingen en dit zowel op het organisatorisch, (bouw)technisch, elektronisch, ICT¹ als op HR² vlak.

Verder willen we nog een dankwoord richten aan alle personen die meegeholpen hebben aan het tot stand komen van deze brochure. Onze bijzondere dank gaat uit naar zowel de diensten van de publieke sector (Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken, Dienst voor Strafrechterlijk Beleid van Federale Overheidsdienst Justitie, de Antiterroristische Gemengde Groepering, de Veiligheid van de Staat, Federale Politie DGJ/DJP/Dienst Terrorisme en Sekten³ waar mijn stage en de realisatie van deze brochure plaatsvond) als naar de veiligheidsverantwoordelijken van enkele bedrijven uit de private sector zonder wiens gewaardeerde medewerking deze brochure nooit tot stand had kunnen komen (Jan Steenlant van het VBO, Dirk Ceulemans van Food Security, Yvan De Mesmaeker van Omega Risk, Paul Robrechts van de Post, Karel Vankeirsbilck van Belgacom, Gilbert Geudens van Carrefour Belgium, Jean-Paul Vandenhoeck van Interbrew, Freddy Pardon van BASF Antwerpen N.V, Bruno De Keyzer en Peter De Meyer van Janssen Pharmaceutica N.V). We wensen ook de stagebegeleider van de KULeuven, Prof Dirk Van Daele, te bedanken voor zijn ondersteunende werking tijdens de stage.

Tenslotte ook nog een dankwoord aan alle andere mensen die ook hun steentje hebben bijgedragen tot de realisatie van deze brochure.

Sara Neven, stagiaire Criminologische Wetenschappen
tweede licentie Katholieke Universiteit Leuven

¹ ICT = Informatie en Communicatie Technologie

² HR = Human Resources

³ DGJ = Algemene Directie Gerechtelijke Politie
DJP = Directie voor de Bestrijding van Criminaliteit tegen Personen

Inleiding

Terrorisme is sedert lang een actueel geopolitiek gegeven. Omdat het onderwerp de laatste jaren niet uit de media was weg te slaan, is er stilaan de bewustwording opgetreden dat er rekening moet worden gehouden met het terrorisme en het extremisme. Niet enkel de overheid of de individuele burger interesseert zich prioritair aan deze veiligheids- en beveiligingsvraagstukken maar ook de private sector voelt aan dat ze een geviseerde doelgroep is voor terroristische groeperingen en derhalve dient rekening te houden met een permanente potentiële terroristische dreiging.

Het risico dat catastrofale terroristische aanslagen gepleegd worden waardoor industriële infrastructuur wordt beschadigd mag niet uit het oog verloren worden. Terroristische en extremistische organisaties zijn zich immers bewust van de impact en het strategisch belang dat een aanslag met zich meebrengt. De gevolgen van zo'n aanval kunnen heel uiteenlopend zijn. De bevolking wordt daarenboven geconfronteerd met onveiligheidsgevoelens. Bovendien zijn de economische en politieke gevolgen tot lange tijd na de aanslag voelbaar voor onze samenleving.

Om beter gewapend te zijn tegen terroristische dreigingen, hebben bedrijven gepoogd om speciale veiligheidsmaatregelen te nemen. Niet enkel via de klassieke fysieke manieren van security, maar tevens door beleidsmatig aan preventiemanagement te doen.

Om deze reden startte er in 2002 onder impuls van de minister van Justitie een permanent overlegplatform tussen de private sector (VBO) en de overheid. Een goede samenwerking tussen deze twee sectoren kan immers constructief bijdragen tot de preventie en bestrijding van het terrorisme.¹

Hieruit vloeide enerzijds een communicatieschema voort tussen de betrokken actoren inzake het terrorisme. Dit informatievierkant of Early Warning System streeft een gestructureerde infolux na, waar informatie kan doorstromen van lokale entiteiten naar federale partners en vice versa.

Anderzijds werd de doelstelling nagestreefd om een brochure te ontwikkelen ten voordele van de private sector met aanbevelingen om zich te beveiligen tegen terroristische dreigingen en misdrijven.²

¹ De samenwerking tussen de private en de publieke sector uit zich naast de werkgroep "terrorisme", ook in de werkgroep "georganiseerde criminaliteit", de werkgroep "bescherming wetenschappelijk en economisch potentieel" en de werkgroep "informaticacriminaliteit".

² DGJ/DJP/DIENST TERRORISME EN SEKTEN, *Rapportering over de uitvoering van het nationaal veiligheidsplan*, Brussel, DGJ/DJP/Dienst Terrorisme en Sekten, 2004, 5.

DEEL 1



Fenomeenanalyse: terrorisme in de bedrijfswereld

DEEL 1

Fenomeenanalyse: terrorisme in de bedrijfswereld

1 Definiëringen van terrorisme

Zowel het Gerechtelijk Wetboek als het Strafwetboek voorziet in definities van terroristische misdrijven.

Het Gerechtelijk Wetboek definieert terrorisme als het gebruik van geweld tegen personen of materiële belangen om ideologische, religieuze of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of bedreigingen te bereiken.¹ Deze definitie staat ook in de wet houdende de regeling van inlichtingen- en veiligheidsdiensten.

Het Belgische strafwetboek voorziet daarenboven, sinds 19 december 2003, in artikels betreffende terroristische misdrijven en groeperingen. Volgens deze wetgeving is een terroristisch misdrijf “een misdrijf dat door zijn aard of context een land of een internationale organisatie ernstig kan schaden en bovendien opzettelijk gepleegd is, met als doel de bevolking angst aan te jagen, de overheid of een internationale organisatie op een onrechtmatige wijze dwingen tot het verrichten of het zich onthouden van handelingen of om politieke, constitutionele, economische of sociale basisstructuren van een land of een internationale organisatie te ontwrichten en te vernietigen”.²

Kenmerkend voor het terrorisme is dat een ander misdrijf als middel wordt gebruikt om een terroristisch doel te bereiken. Een terroristisch misdrijf is bijvoorbeeld een brandstichting die tevens een ideologische, politieke of religieuze boodschap bevat.

Een terroristisch misdrijf kan dus leiden tot een aanzienlijke economische schade. Grootschalige vernieling of beschadiging van infrastructurele voorzieningen zorgen voor verliezen op verschillende domeinen.

Mogelijke acties die terroristen kunnen uitvoeren zijn brandstichting, het tot ontploffing brengen van tuigen, het kapen van transportmiddelen, het laten ontsnappen van gevaarlijke stoffen, het verstoren van de watertoevoer en de

¹ Art. 8.1°, W. 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten en art. 144ter § 1, 2° Gerechtelijk Wetboek, *B.S.* 18 december 1998.

² Art. 137 §1, §2 Sw, ingevoegd bij art. 3 W. 19 december 2003, *B.S.* 29 december 2003.

elektriciteitsvoorziening, bedreiging, ontvoering en gijzelneming van personeel, ...¹
Bovendien kunnen terroristen de productie manipuleren.

Het gevolg is dat vele mensen in (levens)gevaar zijn. Dit alles heeft een grote psychologische impact. Uiteindelijk is niet enkel het bedrijf slachtoffer door structurele en economische schade. Het terrorisme intimideert en victimiseert tevens de sector, de omgeving van het bedrijf, het personeel. Er zijn ook consequenties op het vlak van levering en tewerkstelling. Kortom, terrorisme wekt angst en verbijstering op in de ruimere maatschappij.

De publieke sector maakt doorgaans een onderscheid tussen het nationaal terrorisme en het internationaal terrorisme. De eerste vorm houdt voornamelijk verband met de interessesfeer, de inwoners en het grondgebied van één natie zoals het extreem-links terrorisme, het extreem-rechts terrorisme, het eco-terrorisme evenals het nationalistisch of separatistisch terrorisme. Uiteraard hebben deze fenomenen/groeperingen ook vaak linken met het buitenland, vooral de laatste jaren nu reizen gemakkelijker is geworden en er onder andere via het internet sneller gecommuniceerd kan worden.

Het internationaal terrorisme daarentegen heeft veeleer betrekking op de interessesfeer, de inwoners en het grondgebied van meerdere naties, zoals bijvoorbeeld het islamistisch-radicalistisch terrorisme.²

Verder wordt er aandacht besteed aan bijzondere vormen zoals het NBCR³-terrorisme en het cyberterrorisme.

¹ Art. 137 §1 Sw, ingevoegd bij art. 3 W. 19 december 2003, B.S. 29 december 2003.

² DGJ/DJP/DIENST TERRORISME EN SEKTEN, *Powerpointpresentatie betreffende de Algemene Directie Gerechtelijke Politie; Directie van de bestrijding van de Criminaliteit tegen Personen; Dienst Terrorisme en Sekten*, Brussel, DGJ/DJP/Dienst Terrorisme en Sekten.

³ NBCR = Nuclear Biological Chemical and Radiological

2 Verschijningsvormen

2.1 Algemeen

Niemand kan zeggen dat het fenomeen terrorisme in de goede richting is geëvolueerd. Op 11 maart 2004 vonden er in Europa (Madrid) nog zeer ernstige terroristische aanslagen plaats vanuit islamistisch-radicalistische hoek. De recente aanslagen in London bevestigen deze tendens. Aanslagen in Afrika en Azië tonen aan dat het moslimextremisme ook daar zeer actief en gewelddadig is.

Europa wordt tevens geconfronteerd met brutale terroristische aanslagen van Europees nationalistische origine, zoals in Spanje (ETA) en in Frankrijk (Corsicaanse afscheidingbeweging).

Daarenboven toonden politionele acties in heel Europa aan dat zowel groeperingen van extreem-rechtse als van extreem-linkse strekking niet terugdeinzen om zwaar geweld te gebruiken om hun politieke, religieuze of ideologische doeleinden te bereiken.¹

¹ DGJ/DJP/DIENST TERRORISME EN SEKTEN, *Rapportering over de uitvoering van het nationaal veiligheidsplan*, Brussel, DGJ/DJP/Dienst Terrorisme en Sekten, 2004, 1.

2.2 Terrorisme ten aanzien van de bedrijfswereld

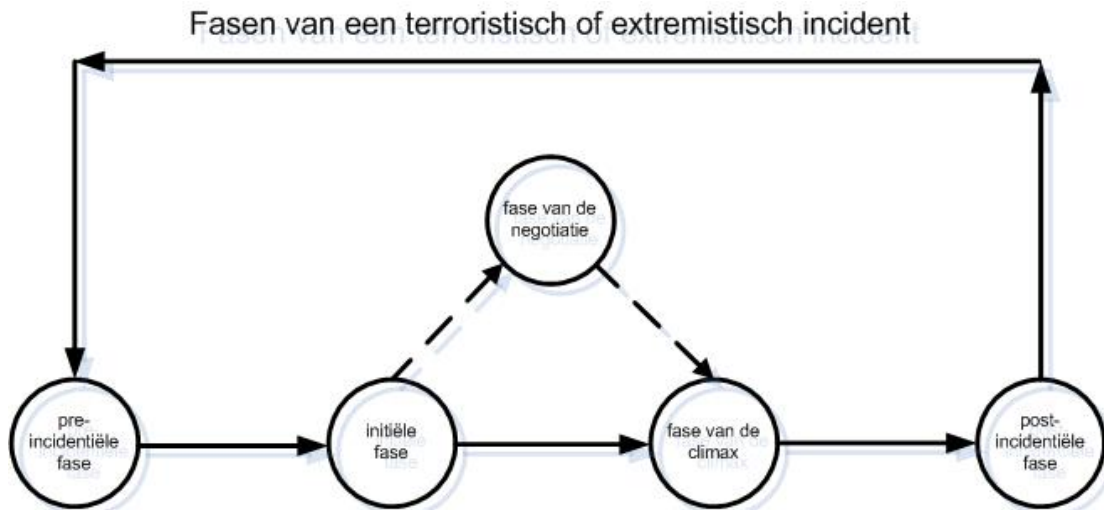
Sommige bedrijven lopen door de specificiteit van de sector, hun “*nationaliteit*”, de aard van hun productieproces, ... meer risico om het slachtoffer te worden van terroristische en extremistische dreigingen of acties.

- Midden de jaren 80 pleegde de CCC¹ verschillende bomaanslagen waarvan één in 1985 gepleegd werd op het gebouw van de Kredietbank in Leuven.
- Het Animal Liberation Front (ALF) organiseerde ecoterroristische acties tegen onder andere fastfoodrestaurants als Quick en Mc Donalds, alsook tegen vleesverwerkende industrieën.
- Recenter werden er in 2003 en 2004 brieven met toxische producten naar verschillende instanties verstuurd per post.
- De laatste jaren uitte SHAC² bedreigingen tegen de farmaceutische, chemische en cosmetische industrie en aanverwanten.
- Wat het cyberterrorisme betreft, kan elke firma vroeg of laat wel eens hinder ondervinden van computervirussen die hun informaticasystemen aantasten. De schade kan enorm zijn wanneer terroristen bepaalde geïnformatiseerde productieprocessen kunnen stilleggen of bepaalde controlerende apparatuur kunnen misleiden (bijvoorbeeld: luchtvaart, betaalverkeer, watervoorzieningen, elektriciteit, ...).
- Verder moet er eveneens gewaakt worden over de voedingsindustrie die gevoelig zou kunnen zijn aan manipulaties met biologische (of chemische) producten.
- Tenslotte is het belangrijk niet uit het oog te verliezen dat de media eveneens een nuttig middel zijn om een terroristisch doel te bereiken. Het gebruik van de media maakt tevens deel uit van de terroristische strijd.

¹ CCC = Cellules Communistes Combattantes

² SHAC = Stop Huntingdon Animal Cruelty. Deze groepering gaat op zoek naar ondernemingen die een link hebben met de onderneming Huntingdon Life Sciences (HLS)

3 Fasen in de organisatie van een terroristisch misdrijf¹



Vooraleer over te gaan tot het plegen van een terroristische aanslag, passen terroristische groeperingen doorgaans een operationele activiteitscyclus toe.

Er zijn verschillende fasen in een terroristische aanval te onderscheiden. Deze fasen zijn belangrijk om te begrijpen welke methoden terroristen hanteren in hun operaties. Dit helpt in de ontwikkeling van preventieve maatregelen.

- Ten eerste is er de *pre-incidentiële of voorbereidingsfase*. In deze fase plant de terrorist zijn acties. In de planningsfase wordt rekening gehouden met doelstellingen op korte en lange termijn. De terroristische organisatie houdt rekening met de eigen mogelijkheden en beperkingen in functie van de vergaarde informatie, de gevoerde observaties én de ervaringen die de groepering reeds in het verleden had. Deze fase van de planning is één van de meest cruciale fasen in de voorbereiding van een terroristische aanslag. De fase neemt een aanvang met de rekrutering van uitvoerders en verdeling van taken. Mogelijke acties die terroristen in deze fase ondernemen zijn voornamelijk het inwinnen van gegevens door: observaties, het zoeken naar de best mogelijke “targets”, het gebruik van informanten, ... De logistieke voorbereidingen omvatten het beschikbaar stellen van transport, het geraken aan de juiste documenten, het verzamelen van wapens en explosieven, ... De private sector kan in deze fase meermaals geconfronteerd worden met

¹ J. FRASER, *Terrorisme: an overview. Clandestine Tactics and Technology. A Technical and Strategic Intelligence Data Service. Is your agency prepared to cope with political violence and*

gewelddadige acties door de terroristen zonder dat deze evenwel aan hen worden toegeschreven. Voornamelijk gaat het hierbij om auto-financieringsoperaties; deze kunnen meerdere vormen aannemen: bijvoorbeeld overvallen (zowel op financiële instellingen als op bedrijven of personen) en afpersingen (de zogenaamde “revolutionaire belasting”), ... Wapen- en voertuigdiefstallen behoren eveneens tot de gebruikte modi operandi. Deze fase gaat men tot in de puntjes uitwerken zodat een succesvolle aanval verzekerd kan worden.

- Ten tweede spreekt men over de *initiële of uitvoeringsfase*. De terroristen beginnen hier aan de operatie. Er is dan geen terugweg meer mogelijk. Men gaat het proces in beweging zetten. Dit is de fase van de eigenlijke terroristische aanslag, meestal opgeëist in naam van de groepering en met bekendmaking van de gestelde eisen of grieven. Terroristen verliezen soms de controle over hun activiteiten in deze fase. Vele onvoorziene gebeurtenissen kunnen in zo'n situatie plaatsvinden en kunnen aan de basis liggen van nog bijkomend geweld.
- De derde fase is de *fase van de negotiatie*. Deze fase komt zelden voor en is zeker niet altijd gepland door de terroristische organisatie. De terroristen kunnen tijdens hun operatie worden gehinderd door de politie. Ze gaan dan alsnog een vluchtweg proberen te vinden. Dit kan leiden tot onderhandelingen tussen de overheid en de terroristische organisatie. Dit garandeert aan de terroristen vaak een grote publiciteit.
- De voorlaatste fase is de *fase van de climax*. In deze fase eindigt het incident. De duur van de beëindiging kan direct na de actie zijn, of kan langer aanslepen bijvoorbeeld bij een gijzeling.
- Tot slot is er de *post-incidentiële fase*. De gevoerde actie wordt hier geëvalueerd en kritisch geanalyseerd. Men gaat conclusies trekken uit zijn handelingen. Deze fase is waardevol bij de voorbereiding van toekomstige aanvallen door de terroristische groeperingen.

DEEL 2



Preventiemanagement

DEEL 2

Preventiemanagement

Uit het eerste gedeelte blijkt dat de private sector wel degelijk het slachtoffer kan worden van terroristische of extremistische acties en dat het zinvol is dat deze private sector zich engageert in de uitwerking van preventieve beveiligingsmaatregelen tegen terrorisme. Behalve het zuiver criminologische aspect, zijn er hiervoor ook nog andere belangrijke redenen:

- de werknemer kent een subjectief veiligheidsgevoel. Na de aanslag van 11 september 2001 in New York is men meer dan ooit gaan inzien dat “de menselijke kant” van het zakendoen ook beschermd moet worden. Denken aan veiligheid, doet ook denken aan personeel en hun mentale noden.
- “het bezig zijn met veiligheid”, geeft eveneens de klant en de aandeelhouder een “veilig” gevoel. Een voorbeeld hiervan is dat na 11 september 2001 de vliegtuigmaatschappijen gingen samenwerken met publieke instanties om een grotere veiligheid te garanderen. Dit had tot gevolg dat de angst van de burger om te reizen met het vliegtuig van relatief korte duur was. Dit alles zorgt op zijn beurt weer voor economische groei en aantrek van nieuwe jobs.¹
- het uitwerken van een goede risico-inschatting bij een dreiging of ten aanzien van een potentiële terroristische aanslag is zeer belangrijk en dit voornamelijk om twee redenen: het kan vooreerst negatieve gevolgen voor de commerciële activiteiten van het bedrijf beperken zoals vb. grote verliezen ten aanzien van de concurrentie, het verlies van de goede reputatie, het failliet gaan van de zaak, het betalen van hogere verzekeringspremies, ...² Daarnaast zal een juiste evaluatie van de dreiging ook beletten dat het bedrijf aan “overacting” gaat doen inzake beschermingsvoorzieningen en de werkomstandigheden niet te fel gehinderd worden.

Uit dit alles blijkt dus dat ieder bedrijf er belang bij heeft om voldoende preventieve maatregelen te nemen ter bescherming tegen mogelijke terroristische (extremistische) acties.

¹ J.N., KAYYEM & P. E., CHANG, *Perspectives on Preparedness: Beyond Business Continuity: The Role of the Private Sector in Preparedness Planning*, s.l., U.S. Department of Justice, 2000, nr 6, 6-7.

² NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world.*, London, London First, 2003, 3.

1 Preventie

Volgens Dhr. Muller heeft preventie betrekking op maatregelen die genomen kunnen worden om potentiële dreigingen van terrorisme en extremistische acties te doen verminderen of zelfs te doen verdwijnen.¹ Het is een weloverwogen proces dat tot doel heeft inzicht te verkrijgen in de risico's, op basis waarvan wordt besloten welke maatregelen zullen worden genomen en ten uitvoer gelegd om het risico tegen een aanvaardbare prijs tot een bepaald niveau te reduceren. Het doel van deze benadering is dus de risico's te onderkennen, in te schatten en tot een bepaald niveau te beperken.² De algemene context van het terrorisme en de internationale actualiteit zoals in het vorige hoofdstuk werd beschreven zal één van de pijlers zijn die kan bijdragen tot een degelijke risicoanalyse.

Het Nationaal Veiligheidsplan van de Federale Politie stelt als strategische doelstelling bij te dragen tot het voorkomen van terroristische aanslagen. Er moet getracht worden voorbereidende activiteiten, gesteld op Belgisch grondgebied, te ontdekken en er gepast tegen op te treden. De terroristische groeperingen actief op het Belgische grondgebied moeten gedestabiliseerd worden.³

De inschatting of de evaluatie van de potentiële dreiging uitgaande van terroristische groeperingen in België en tegen Belgische belangen (zowel officiële als private) in het buitenland is door de regering toegewezen aan de Antiterroristische Gemengde Groep (AGG), opgericht op 17 september 1984 (K.B. van 17 oktober 1991). Deze evaluatie wordt opgemaakt aan de hand van de gegevens, aangeleverd door diensten, vertegenwoordigd in de AGG, te weten de Geïntegreerde Politie, de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid (ADIV) van het leger, alsook ingezameld via open en gesloten bronnen uit binnen- en buitenland. Het betreft zowel globale (strategische) evaluaties als punctuele (operationele) evaluaties. De punctuele of operationele evaluaties vinden grotendeels plaats op vraag van de Algemene Directie Crisiscentrum (ADCC⁴) van de Federale

¹ E.R. MULLER, *Terrorisme en terreurbestrijding na 11 september 2001*, in B. PATTYN en J. WOUTERS (ed.), *Schokgolven. Terrorisme en fundamentalisme*, Leuven, Davidsfonds, 2002, 26-31.

² COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Terrorismebestrijding: bescherming van kritieke infrastructuur*, Brussel, Commissie van de Europese Gemeenschappen, 2004, 6.

³ DGJ/DJP/DIENST TERRORISME EN SEKTEN, *Rapportering over de uitvoering van het nationaal veiligheidsplan*, Brussel, DGJ/DJP/Dienst Terrorisme en Sekten, 2004, 1.

⁴ ADCC = de bevoegde overheidsdienst die namens de Minister van Binnenlandse Zaken beslist welke maatregelen van bestuurlijke politie dienen te worden genomen ter bescherming van personen en

Overheidsdienst Binnenlandse Zaken (K.B. van 18 april 1988 tot de oprichting van het Coördinatie- en Crisiscentrum van de Regering, B.S. 4 mei 1988, gewijzigd bij K.B. van 11 mei 1990, B.S. 1 juni 1990).

Om dit alles te bereiken is dus een goede samenwerking tussen de private en de publieke sector wenselijk en kan deze constructief bijdragen tot de preventie en de bestrijding van het terrorisme. Om deze reden werden er reeds informatiekanalen ontwikkeld om relevante informatie uit te wisselen (cf. Voorwoord en inleiding).

2 Risicoanalyse door het bedrijf

Om tot een adequate risicoanalyse te komen, is het belangrijk dat het bedrijf een goede inschatting kan maken van de dreiging door onder andere zichzelf goed te situeren binnen de algemene (geo)politieke context, en dat ze eveneens een goed beeld probeert te vormen van de schade die dergelijke dreiging kan creëren.



instellingen in het land en daartoe aan de politiediensten de nodige instructies geeft (instellingen www.crisis.ibz.be).

2.1 Dreigingsanalyse

Om te weten hoe groot het risico is dat een bepaald bedrijf het slachtoffer kan worden van terrorisme is het nodig om eerst een dreigingsanalyse op te stellen. Door de sterktes en zwaktes van de onderneming in te schatten, kan men de balans maken hoe groot de kans is om het slachtoffer te worden van een mogelijke terroristische actie.

Het is aan te raden om het personeel in deze stap te betrekken zodat ze zich betrokken voelen. In sommige gevallen is het nuttig om in deze fase van de analyse van het bedrijf reeds een expert inzake preventie, beveiliging en veiligheid te raadplegen. Deze analyseert immers de onderneming op een objectieve wijze, wat ongetwijfeld zorgt voor een meerwaarde in het Business Continuityplan (cf. infra).

Verder moet er nagegaan worden of het bedrijf reeds crisisplannen heeft die rekening houden met mogelijke terroristische acties. Deze plannen moeten kritisch geanalyseerd worden. Aspecten die herbruikbaar zijn, kunnen opgenomen worden in het nieuwe businessplan.

In deze fase is het dus vooral noodzakelijk dat het bedrijf zichzelf leert “begrijpen”¹:

- het is nuttig na te gaan of de bedrijfssector is opgenomen in de lijst van de Kritieke Nationale Infrastructuur, op federaal niveau voorhanden bij de Commissie voor de Nationale Vraagstukken inzake Verdediging (CNVV), die deel uitmaakt van de ADCC. Dit geldt ook voor bedrijven die in de buurt van deze kritieke, vitale of sensibele sectoren gevestigd zijn. Immers, doordat ze een “buur” zijn van zo’n bedrijf, lopen ze mogelijk een verhoogd risico om medeslachtoffer te worden van terroristische of extremistische acties;
- er dient aandacht te worden besteed aan de aard en de duur van de productieprocessen (vb. grondstoffen die in de kijker staan bij sommige extremistische groeperingen, zoals genetisch gemanipuleerde organismen, producten uitgetest op dieren, bont, ganzenlever, vleesverwerking, ...). Ook dient er geverifieerd te worden of dergelijke productieprocessen in het verleden reeds het voorwerp hebben uitgemaakt van dreigingen of acties, eventueel zelfs in het buitenland;

¹ NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world.*, London, London First, 2003, 6-8.

- bovendien is het zinvol om na te gaan hoe de interne interacties tussen het personeel, de zakenpartners, de leveranciers en de klanten verlopen (Werden klanten of leveranciers reeds eerder geïdентificeerd door extremistische groeperingen?);
- de structuur en de infrastructuur van de gebouwen dient ook kritisch bekeken te worden (vb. ligging aan een haven, ingangen, controleposten, ...);
- tenslotte is het noodzakelijk dat het bedrijf zich kan situeren in de (geo)politieke context. De onderneming zou moeten rekening houden met de uitstraling die het heeft bij bepaalde extremistische groeperingen (banken als symbool van het kapitalisme, olieverwerkende nijverheid, ...). Sommige bedrijven lopen immers meer in de kijker bij extremistische groeperingen door de aard van hun productieproces of hun afgeleverde of verkochte producten (bijvoorbeeld producten uit het Midden-Oosten, ...).

2.2 Risicoanalyse

Bij de inschatting van de risico's moet worden getracht te identificeren door welke bedreigingen het bedrijf het meest geïdентificeerd kan worden, wat is de kans dat zo'n bedreiging kan worden voorkomen en welke effecten dit mogelijk kan hebben op het bedrijf.¹ Op deze manier kan een onderneming inschatten wanneer ze bijkomende veiligheidsmaatregelen moet treffen². Idealiter houden bedrijven ook steeds rekening met een "worst case scenario".³

In de praktijk wordt er best een matrix opgemaakt waarin de variabelen "ernst van de mogelijke schade" en "waarschijnlijkheid of dreiging" met elkaar vergeleken worden. Hoe groter de graad van de "ernst van de mogelijke schade" en de graad van "waarschijnlijkheid of dreiging" is, des te groter is het risico. De toepassing van risicomanagement maakt het mogelijk de aandacht toe te spitsen op die gebieden waar het risico het grootst is. Dit impliceert een verhoogde waakzaamheid wat zou moeten leiden tot meer en specifieke preventieve maatregelen.⁴

¹ NATIONAL COUNTER TERRORISM SECURITY OFFICE, *Expecting the unexpected. Business continuity in an uncertain world.*, London, London First, 2003, 10.

² D.A., MOORE, *Powerpointpresentatie: The Challenge of Making Risk Decisions for Port Security*, Antwerpen/San Francisco, AcuTech Consulting Group, 2004.

³ NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 2003, 10.

⁴ *Ibid.*, 10.

Uit de risicoanalyse kan dan al dan niet worden afgeleid of een firma tot de industriële kritieke infrastructuur behoort. Kritieke infrastructuur zijn netwerken of aanvoerketens voor de continue levering van een belangrijk product of essentiële dienstverlening. Een vernietiging of verstoring van infrastructuur van materiële en informatietechnologische voorzieningen, netwerken, diensten en activa kan ernstige gevolgen hebben¹ en dit niet alleen voor het getroffen bedrijf, maar eveneens voor de ondernemingen die in de nabije omgeving liggen of zelfs dezelfde infrastructuur delen, en/of via het productieproces afhankelijk of onderling verweven zijn (het zogenaamde domino-effect: wanneer door een aanval de stroomvoorziening uitvalt, kan bijvoorbeeld ook de turbine van de watervoorziening uitvallen). Zo maakt bijvoorbeeld een geslaagde cyberaanval weinig of zelfs geen slachtoffers, maar kan deze er wel voor zorgen dat vitale infrastructurele diensten kunnen uitvallen. Een geslaagde aanval op het telefoonnet kan cliënten ontnemen om te telefoneren. Een aanval op het besturingssysteem van een chemische installatie of van een aardgasinstallatie zou tot een groter verlies en tot aanzienlijke materiële schade kunnen leiden.²

Globaliter kunnen we de gevolgen indelen in vijf categorieën:³

- gevolgen voor de bevolking (dodelijke slachtoffers, gekwetste personen, ziekten, secundaire victimisering, evacuatieproblemen, psychologische factoren zoals traumatisering, dramatisering van gebeurtenissen, ...);
- gevolgen voor het milieu;
- economische gevolgen (omvang van het economische verlies en/of daling van de kwaliteit van producten of diensten, onrechtstreekse gevolgen voor het Bruto Binnenlands Product);
- politieke gevolgen;
- gevolgen die een combinatie vormen met één of meer aspecten uit de voorgaande categorieën.

Uiteraard zullen we later in onze “strategie” moeten rekening houden met het feit dat niet alle infrastructuren tegen alle dreigingen kunnen worden beschermd. Sommige voorzieningsnetwerken zoals bijvoorbeeld de stroomverdeling zijn te omvangrijk om te worden omheind of bewaakt.⁴

¹ COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *Terrorismebestrijding: bescherming van kritieke infrastructuur*, Brussel, Commissie van de Europese Gemeenschappen, 2004, 4.

² Ibid., 3.

³ COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *o.c.*, 5-6.

⁴ Ibid., 6.

3 Het ontwikkelen van een strategie

Uit het voorgaande blijkt dat er dus zowel dient rekening gehouden te worden met de dreiging, het risico of zelfs de mate waarin de infrastructuur als kritiek kan worden beschouwd en het bestaande beschermingsniveau. Dit alles moet ons leiden tot het volgen van een bepaalde strategie om de gevolgen op te vangen en de continuïteit van de bedrijvigheid te garanderen, in overeenstemming met de mogelijkheden en de visie van het bedrijf.¹ Aan de hand van de risicoanalyse, kan er nu een keuze gemaakt worden uit de volgende strategieën:²

- het bedrijf kan de risico's aanvaarden en beslissen om niets te veranderen;
- het bedrijf kan beslissen om zichzelf geen interne maatregelen op te leggen, maar een partnerschap af te sluiten met andere bedrijven/instellingen die op basis van een opgebouwde expertise eventueel kunnen adviseren na een incident;
- de onderneming kan beslissen om (bijkomende) maatregelen te treffen om de risico's te reduceren en te vermijden;
- de onderneming heeft de mogelijkheid om zelf enkele maatregelen te treffen, maar gaat tevens contact opnemen met partners (incl. overheid), zodat er zeker expertise aanwezig zal zijn wanneer een incident zich toch voordoet;
- de onderneming kan trachten de risico's zo sterk te reduceren dat het naar een punt wordt herleid dat het bedrijf alle risico's zelf kan opvangen en hulp van buitenaf overbodig lijkt.

¹ COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *o.c.*, 2004, 6.

² NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 14-16.

4 Het ontwikkelen van het plan

4.1 Business Continuityplan: situering

Op basis van de strategische benadering moet er nu via de ontwikkeling van een managementplan gedacht worden aan welke maatregelen er vóór (preventieve), tijdens (acties die ondernomen moeten worden tijdens de incidentieperiode) en na (heropbouwbeleid) de “terroristische actie” kunnen genomen worden.

Dit laatste aspect wordt wel eens over het hoofd gezien. Een Business Continuityplan helpt een bedrijf met de voorbereiding om noodgevallen en “onverwachte situaties” te overbruggen. Het doel van de planning is om zo snel mogelijk terug te kunnen overgaan naar de “normale gang van zaken”. Business Continuity Management kan dus best gedefinieerd worden als “een holistisch managementproces dat de potentiële impact van een (terroristische) dreiging naar een organisatie toe tracht te identificeren. Het reikt een handvat aan rond hoe er op een effectieve manier respons kan gegeven worden ten aanzien van mogelijke dreigingen en aanvallen die zich (vanuit terroristische hoek) tegen een bedrijf kunnen richten”.¹

Business Continuitymanagement is zowel voor kleine als voor grote bedrijven zinvol. De planmatige aanpak zorgt ervoor dat via een eenvoudige maar effectieve manier naar de noden van de organisatie wordt gekeken. Door het hanteren van een gedetailleerd stappenplan worden er geen cruciale componenten over het hoofd gezien. Wanneer er zich een incident voordoet, reduceert dit de negatieve impact op het (economische) welzijn van het bedrijf.²

¹ NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 2.

² D. BLUNKETT, *Expecting the unexpected. Business continuity in an uncertain world.*, London, London First (National Counter Terrorism Security Office), 2003, 1.

4.2 Business Continuityplan: invulling¹

Business Continuityplannen verschillen van bedrijf tot bedrijf, maar toch worden in goede plannen vaak dezelfde basiscomponenten terug gevonden. Een plan moet zowel strategisch², tactisch³ en operationeel⁴ goed in elkaar zitten.

- Belangrijk is dat bij de ontwikkeling van een plan alle afdelingen van het bedrijf geconsulteerd worden.
- Het plan bevat best een eenvoudig taalgebruik dat verstaanbaar is voor iedereen. Het is ingebed in een eenvoudige structuur. Het is nooit mogelijk om elk detail te overzien. Het belangrijkste is dat men weet hoe men snel en adequaat kan reageren in een noodgeval.
- Er moet duidelijk vermeld worden wie in bepaalde situaties welke acties onderneemt. Maak een checklist van de maatregelen en instructies die genomen moeten worden gedurende de eerste cruciale uren na het incident (standaardprocedures). Bijvoorbeeld: wie contacteert de lokale politie? Gebruik een schematische vorm met onderdelen in puntjes die gemakkelijk te overlopen zijn.
- Bij de ontwikkeling van een plan is het nodig om het plan op het voorhand te checken, en daar waar nodig bij te sturen. Het plan moet ook regelmatig geëvalueerd worden zodat het up to date blijft en steeds aangepast is aan de risico's.
- Idealiter wordt er ook rekening gehouden met het "worst case scenario". Zo zou het plan kunnen voorzien in een locatie waar de bedrijvigheid kan worden verder gezet.

¹ NATIONAL COUNTER TERRORISM SECURITY OFFICE, *o.c.*, 18-21.

² Strategisch = bekwaamheid om met behulp van de ter beschikking staande middelen een gesteld doel, of plan van handelen te bereiken.

³ Tactisch = op de meest gepaste manier te werk gaan om te slagen in het vooropgestelde doel of het plan van handelen.

⁴ Operationeel = dat het vooropgestelde doel, of het plan van handelen klaar voor gebruik, werkbaar en toepasbaar is.

5 Evaluatie van het plan

Door de realisatie van het preventieplan, is de oefening evenwel nog niet beëindigd. Een plan is een document dat voortdurend bijgestuurd moet worden. Derhalve raden wij aan uw veiligheidsplannen actief uit te voeren, geregeld inspecties en oefeningen te organiseren en deze grondig te evalueren.¹ Het regelmatig testen van het plan houdt het “up to date”. Zwakten en leemtes kunnen zo ontdekt en bijgestuurd worden.

6 Conclusie

Een planmatige behandeling van veiligheid ten aanzien van terrorisme zet aan tot een samenbundeling van de krachten tussen de private en publieke sector. Door een proactieve samenwerking tussen de private en de publieke sector kunnen de verschillende actoren die deel uitmaken van het economisch proces beschermd worden.²

Alleszins is het de bedrijven aangeraden om een Business Continuityplan op te stellen zodat gelet op de eigen zwakten en sterkten met het oog op een betere werking en het waarborg van de continuïteit.

¹ COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN, *o.c.*, 10.

² D. BLUNKETT, *o.c.*, 1.

DEEL 3



Preventieve maatregelen

DEEL 3

Preventieve maatregelen

Dit gedeelte vormt de concretisering van de twee voorgaande delen, waar we proberen tips, maatregelen en aanbevelingen mee te geven zodat een onderneming zich beter kan beschermen ten aanzien van terroristische dreigingen en/of acties. Zoals reeds gesteld, een succesvol preventief antwoord op een concrete of een potentiële terroristische actie hangt af van de kwaliteit van het Business Continuityplan met de beveiligingsmaatregelen. Uiteraard, quasi alle maatregelen die kunnen worden genomen in het kader van terrorisme zijn ook van toepassing op de meeste andere criminaliteitsfenomenen.

Deze beveiligingsmaatregelen kunnen diverse vormen aannemen.

Gezien de vaak beperkte middelen moet er via een goede kosten-batenanalyse naar een ideale balans gestreefd worden tussen de risico's en de beveiligingsmaatregelen. Immers, bij het nemen van maatregelen wordt te vaak onmiddellijk gedacht aan technische oplossingen en dure investeringen. Een dergelijke benadering leidt er vaak toe dat eenvoudige, organisatorische maatregelen worden vergeten, waardoor de effectiviteit van de vaak dure technische uitrusting tekort schiet. Daarbij komt nog dat de kosten redelijk hoog zijn in vergelijking met de beperking van het risico.

Idealiter komt de nadruk in het beveiligingsplan veeleer te liggen op kwaliteits- en organisatieaspecten zoals betrokkenheid van werknemers, verantwoordelijkheid, communicatie en motivatie; deze hebben dikwijls een grotere efficiëntie dan de dure technische en elektronische voorzieningen.

Verder, een samenwerking tussen de private en de publieke sector vergemakkelijkt het preventieproces ten aanzien van terrorisme.¹

Om risico's voor terroristische of extremistische acties zoveel mogelijk te vermijden, is het best dat er verschillende maatregelen naast elkaar worden gebruikt. Deze maatregelen kunnen uiteraard sterk variëren van onderneming tot onderneming, maar de volgende aanbevelingen hebben een algemeen karakter zodat ze zouden kunnen worden vertaald naar elke onderneming.²

¹ J. WILLEMS, *Terrorisme en scheepvaart*, Antwerpen, Federale Politie: DGA/DAC/SPN/SPN-Antwerpen, 2004, 27.

² FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *Veilig zelfstandig ondernemen*, Brussel, DIE KEURE, Algemene Directie Veiligheids- en Preventiebeleid, Vast Secretariaat voor het Preventiebeleid, 2004, 44.

De maatregelen die kunnen worden gehanteerd om een betere preventie ten aanzien van terroristische of extremistische acties te garanderen kunnen we naar *aard* onderscheiden in 5 verschillende categorieën: *organisatorische*, *(bouw)technische*, *elektronische*, *ICT-*, en *personele (HR)* maatregelen. In deze volgorde zijn de maatregelen het meest effectief. De kosten van de elektronische middelen zijn veelal het hoogst, terwijl de organisatorische maatregelen nagenoeg geen kosten met zich meebrengen.¹ Hierbij moet nog vermeld worden dat sommige preventieve maatregelen onder meerdere categorieën zouden kunnen geplaatst worden.

1 Organisatorische maatregelen

Organisatorische maatregelen kunnen als prioritair worden beschouwd. Aldus, in geval van een probleem of een incident, raden we aan niet naar een onmiddellijke oplossing te zoeken voor dat specifieke probleem, zonder in te gaan op de diepere oorzaken. Immers, de oorzaak ligt vaak niet in het falen van technische beveiligingsapparatuur, maar wel in de gebrekkige aandacht voor preventie binnen de onderneming.² Daarenboven kosten deze organisatorische maatregelen (inzet van de onderneming en zijn personeel) relatief weinig.

Voorbeelden van zulke organisatorische maatregelen zijn onder andere het opmaken van een evacuatieplan om het bedrijf zo snel mogelijk te kunnen ontruimen, of het nadenken over wat men kan doen in afwachting van mogelijke (professionele) hulp.

1.1 Sensibiliseringsacties en trainingen voor werknemers

Het veiligheidsbeleid moet een duidelijke plaats krijgen in de dagelijkse praktijk. Veiligheid moet een regelmatig thema zijn in de besprekingen met het personeel. Het kan soms nuttig zijn om trainingen en sensibiliseringsacties opens bepaalde securityrisico's te organiseren. Op deze manier leert het personeel van de onderneming herkenningcriteria te onderscheiden. Zo wordt het risicobewustzijn en een veiligheidsreflex gestimuleerd bij elke werknemer. Duidelijke afspraken voor de melding en de centralisatie van veiligheidsincidenten zijn belangrijk. De instructies

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 15, 30.

² *Ibid.*, 40.

van en voor het personeel worden best kort en helder geformuleerd. Belangrijke telefoonnummers moeten duidelijk zichtbaar worden aangegeven.¹

Zulke acties kunnen op verschillende manieren georganiseerd worden. Via posters, folders en mails op het intra- en internet kan het personeel gesensibiliseerd worden. Deze acties kunnen bijvoorbeeld door de communicatiedienst binnen het bedrijf georganiseerd worden, of door externe firma's die ingehuurd worden om zulke sessies te houden.

1.2 Kwaliteitscontroles op het product

Door op regelmatige basis kwaliteitscontroles uit te voeren, kan het bedrijf manipulaties van terroristische of extremistische aard aan de bron ontdekken. Immers, wanneer terroristen op de hoogte zijn dat de onderneming regelmatig steekproeven verricht naar de kwaliteit van de producten in de verschillende fasen van het productieproces, zullen sommigen mogelijk minder geneigd zijn om dit productieproces te manipuleren. Daarenboven kan hiermee voorkomen worden dat het gemanipuleerde product slachtoffers maakt en/of de media haalt. Uiteraard zal de “*doorwinterde actievoerder*” zich hierdoor niet laten afschrikken.

1.3 Overzichtelijke bedrijfsinrichting en ordelijke huishouding

Wanneer het bedrijf een ordelijke en beheerste uitstraling heeft (intern en extern), is de kans groter dat ongewenste bezoekers opgemerkt worden.

Binnen de muren van de onderneming wordt best een goed overzicht bewaard. Een goede verlichting is aangewezen teneinde donkere plaatsen en hoeken te vermijden. Ook de uitstraling buiten het bedrijf is van belang. Zo wordt de omgeving, vb de parking, best ordelijk, net en overzichtelijk gehouden.

1.4 In- en uitgangen

Het aantal in- en uitgangen wordt best tot een minimum beperkt.

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 51, 57.

1.5 Toegangswegen^{1 2}

Er moet vermeden worden dat klanten, bezoekers en leveranciers ongezien de onderneming betreden. Bezoekers moeten steeds het gevoel hebben dat ze gezien kunnen worden.

De meest effectieve manier is dat er enkel toegang kan gegeven worden via de aanmelding van de bezoeker, klant of leverancier aan een receptie waar ze worden begroet. Deze krijgt dan nadat checken of de afspraak of levering diende te gebeuren, de toestemming om (liefst met een badge) het bedrijfsterrein te betreden. Voor het eigen personeel is het gemakkelijk om een geïnformatiseerde badge met foto te laten ontwikkelen. Door de informatisering van de badge, kan ervoor gezorgd worden dat er enkel aan bepaalde plaatsen toegang wordt verleend voor bepaalde werknemers.

Wanneer er geen receptie is kan er geopteerd worden voor het filmen van de bezoekers aan de ingang. Via een digitale camera worden de beelden dan naar een interne monitor gestuurd. Zo kan beslist worden om de bezoeker, klant of leverancier al dan niet te ontvangen.

Bezoekers worden best vergezeld door iemand van het bedrijf, of door iemand van de interne veiligheid en dit idealiter enkel in ruimtes die toegankelijk zijn voor alle werknemers. Deze ruimtes worden best steeds gesloten en/of gecontroleerd. Ze dragen best een toegangsbadge, die ze terug moeten afgeven bij het verlaten van het gebouw. Ongewenste bezoekers kunnen opgemerkt worden, wanneer men ziet dat deze persoon niet begeleid is en/of geen pasje heeft.

In sommige gevallen is het aangeraden om binnen de marges van de wettelijke mogelijkheden de bagage of de te leveren goederen te checken alvorens ingang tot het bedrijf te verschaffen. De receptie dient tevens voorzichtig te zijn wanneer onaangekondigde bezoekers zich aanmelden.

¹ HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers*, s.l., Home Office, s.d., 11.

² Opgelet ! Bij toegangs- en uitgangscntroles evenals identiteitscontroles, moet rekening worden gehouden met de wetgeving inzake private veiligheid : zie <http://www.vigilis.be> ; ook de regelgeving inzake bescherming van de persoonlijke levenssfeer moet worden in acht genomen, bv. voor wat betreft cameratoezicht : zie <http://www.privacy.fgov.be>

1.6 Zichtbaar optreden in de onderneming¹

Gedragbeïnvloedende maatregelen hebben effect op het afschrikken van terroristen. Wanneer het personeel strategisch opgesteld is, kan er op elke plaats van de onderneming toezicht zijn. *Camera's* staan best op zowel zichtbare als onzichtbare plaatsen. Potentiële terroristen gaan namelijk gemakkelijker acties ondernemen op plaatsen waar ze niet gezien en/of gefilmd kunnen worden. Goedkopere nepsystemen kunnen een alternatief zijn, maar hebben een minder grote effectiviteit op lange termijn.

Toezicht door (*geüniformeerde*) personen (eventueel van externe beveiligingsfirma's) schrikken "minder betrouwbare" klanten en leveranciers af. Werknemers worden best duidelijk herkend aan een aangepast uniform of gepersonaliseerde badge. Het cliënteel, leveranciers en bezoekers mogen duidelijk merken dat de zaak beveiligd is. Op deze manier beseffen bezoekers dat de pakkans bij het opmerken van verdachte situaties reëel is.

1.7 Contact met cliënteel, bezoekers en leveranciers

Het is ten zeerste af te raden om klanten gevoelige informatie te geven over geldtransacties, beveiligingsmaatregelen of bepaalde veiligheidsprocedures die gehanteerd worden in de firma.

1.8 Sleutelplan en sleutelbeheer²

De onderneming moet een *sleutelplan* opstellen. Dit sleutelplan kan bevatten:

- welke ramen, deuren en kasten een slot hebben;
- op welke tijdstippen er moet afgesloten worden;
- wie er bevoegd is om bepaalde ruimtes te betreden;
- wie de verantwoordelijke is voor het afsluiten van specifiek beveiligde ruimtes;
- wie de sleutels bewaart op welke plaatsen;
- welk type van sluiting zal worden gebruikt (sleutel of code);

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, o.c.,44-48

² FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, o.c., 49-53.

- wat de exacte procedure is voor het afsluiten.

Het *sleutelbeheer* daarentegen omvat het geheel van procedures om sleutels efficiënt en veilig te bewaren. Situaties waarbij er sleutels onbeheerd achterblijven of in het bezit zijn van te veel verschillende personen, moeten worden vermeden.

Enkele aanbevolen maatregelen zijn:

- het aantal personen die sleutels bezitten, moet beperkt worden tot een strikt minimum;
- reservesleutels moeten bewaard worden op een veilige plaats waar onbevoegden geen toegang tot hebben;
- er worden geen labels op de sleutels aangebracht: zo kan immers iedereen weten welke sleutel op welk slot past. Een alternatief is de sleutels nummeren of ze van een kleurcode voorzien;
- personen die (een) sleutel(s) hebben ontvangen, kan men laten handtekenen bij ontvangst;
- bij diefstal of verlies van een sleutel is het verplicht dit onmiddellijk te melden;
- sleutels worden niet aan tijdelijke krachten overhandigd;
- veiligheidscilinders hebben veiligheidssleutels; zonder voorlegging van een certificaat kunnen geen sleutels worden bijgemaakt omdat het profiel beschermd is;
- een verantwoordelijke moet worden aangeduid voor het sluiten van de onderneming en de regelmatige controle van het hang- en sluitwerk (werking, beschadiging, ...) bij het verlaten van de zaak;
- indien er een alarmsysteem is, kan het personeel hiervan op de hoogte gebracht worden. Hoe het alarm wordt ingeschakeld, dient eveneens meegedeeld te worden aan de personeelsleden, terwijl de uitschakeling beter beperkt wordt tot de verantwoordelijke(n) voor het openen en sluiten.

Verder dient men alert te zijn bij het openen en sluiten van de onderneming. Er moet opmerkzaamheid geboden worden zodat verdachte personen of omstandigheden kunnen opgemerkt worden. De toegang moet voldoende overzicht bieden op de omgeving en is best goed verlicht. Voor de totale afsluiting moet de hele onderneming gecontroleerd worden op eventuele "achterblijvers".

1.9 Bommelding¹

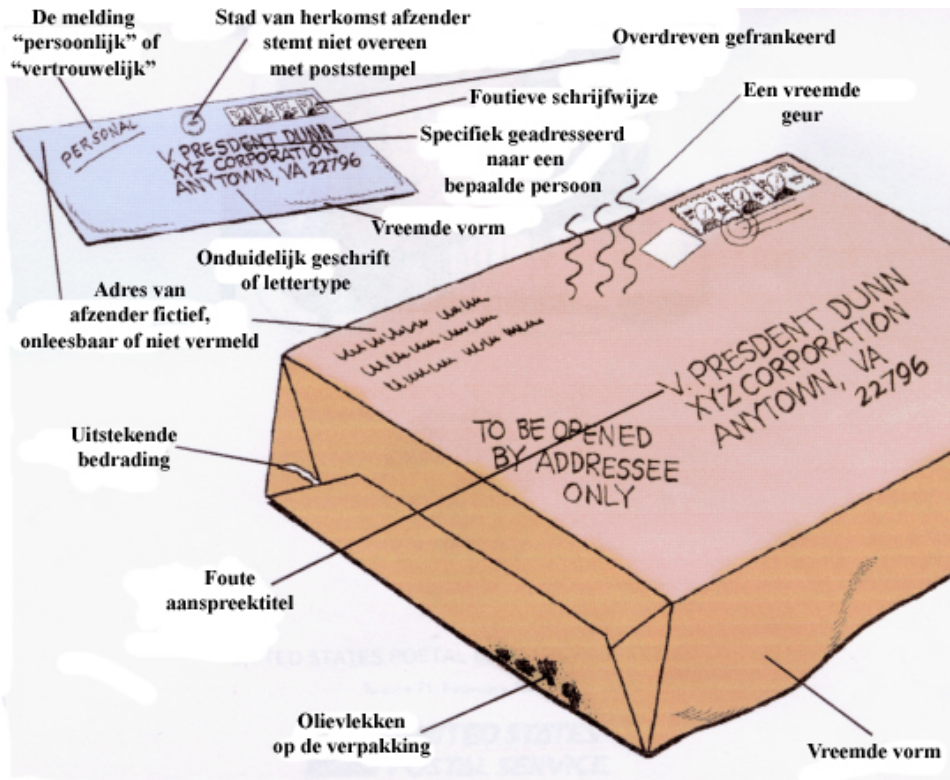
Wanneer een bedrijf geconfronteerd wordt met een bomalarm is het moeilijk om kalm en effectief te reageren. Er moeten dan acht gouden regels gehanteerd worden.

- rustig blijven;
- probeer zoveel mogelijk informatie van de beller te vergaren (geslacht, motief,...). Hou hem aan de lijn en noteer alles wat hij zegt;
- meld de bommelding meteen aan de veiligheidsverantwoordelijke van het bedrijf en verwittig onmiddellijk de politie. Het bedrijf is in principe niet wettelijk verplicht om de politie in te lichten van de bommelding. Wanneer het echter geen “vals alarm” is en er bijgevolg veel schade kan opgelopen worden, kan het bedrijf eventueel verantwoordelijk worden gesteld voor het verzuim van de bommelding. Hierbij moet tevens opgemerkt worden dat het melden van het bomalarm aan de politieke instanties niet automatisch wil zeggen dat het productieproces zal worden stilgelegd.
- als u bent ingelicht over de bommelding, raak dan geen verdachte pakketten aan;
- gebruik een checklist zodat geen acties over het hoofd worden gezien. De checklist moet op een plaats liggen waar hij onmiddellijk beschikbaar is;
- sta bij de evacuatie nooit voor een raam of een glazen deur;
- blokkeer geen wegen die kunnen dienen als vluchtweg;
- voorzie in een vooraf bepaalde plaats waar het personeel zich kan verzamelen bij evacuatie. We raden u wel aan deze te veranderen na een incident, daar het in het verleden reeds is gebeurd dat bij een bomalarm ook deze evacuatieplaats werd getroffen door een explosie.

Het is zinvol om regelmatig een simulatieoefening te houden betreffende het bomalarm. Op deze manier kan de evacuatie getest worden en kunnen knelpunten bijgewerkt worden.

¹ N. SCHOOF, *Bommen op kantoor*, www.vacature.com, 21.08.2004
HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers*, s.l., Home Office, 10.

1.10 Verdachte zendingen (en verdachte voertuigen)¹



Postpakketten en brieven worden best in een afgesloten ruimte door een ervaren personeelslid gesorteerd. Wanneer men denkt dat het om een *poederbrief* gaat, gelden volgende raadgevingen:

- de brief niet schudden, noch enige andere vorm van manipulatie; de zending mag niet geopend worden, ook niet gedeeltelijk. Ieder onnodig contact met de zending moet vermeden worden;
- het stuk moet apart geplaatst worden, minimaal in een plastic zak (idealiter opbergen in twee hermetisch afgesloten plastic zakken) teneinde "verspreiding" te voorkomen; bij gebrek aan een plastic zak of enige andere vorm van omhulsel, zorg dat niemand anders de zending kan manipuleren;
- de ruimte moet geëvacueerd worden en afgesloten voor anderen;
- ventilatie moet vermeden worden en de airconditioning moet stil gelegd worden;

¹ DGJ/DJP/DIENST TERRORISME EN SEKTEN, *Colis piégés – éléments d'appréciation et recommandations*, Brussel., DGJ/DJP/DIENST TERRORISME EN SEKTEN,s.d., 1-4.

- indien poeder werd gemorst, kuis dit niet op maar bedek het met een kledingstuk, papier e.d. ter vermijding van verdere verspreiding;
- personen die in contact kwamen met het product dienen grondig de lichaamsdelen die in contact kwamen met het product met water en zeep te wassen.

In het geval van een *bombrief of bompakket*:

- raak het pakket niet aan, tracht zoveel mogelijk details te memoriseren;
- de brief moet rustig gehanteerd worden, trillingen moeten vermeden worden, de plaats moet verlaten worden en eventueel aanwezige collega's moeten meegenomen worden;
- de plaats moet afgesloten worden; dit zorgt ervoor dat ze niet meer door andere collega's kan worden betreden;
- er moet een perimeter ingezet worden in de omgeving, zodat er een "bewaking" op afstand is;
- gebruik geen GSM, draagbare radio's of dergelijke.

In het geval van een *verdacht voertuig*:

- dezelfde reflexen als bij het voorgaande dienen gehanteerd te worden. Een perimeter van ongeveer 200 meter dient in overweging genomen te worden.

Een *verdacht postpakket en verdachte brieven* kunnen ontdekt worden door:

- vreemde vorm en/of ongebruikelijk gewicht;
- manipulatie geeft een andere indruk dan bij papier het geval zou zijn;
- ongebruikelijke hoeveelheden kleefband werden gebruikt;
- vetvlekken of verkleuringen op het postpakket (eventueel door poeder);
- het adres van de afzender is niet vermeld, onleesbaar of oncontroleerbaar;
- de brief is onverwacht en/of van een totaal onbekende/ongebruikelijke afzender;
- het land/de stad van herkomst van de afzender van de briefwisseling stemt niet overeen met de poststempel;
- in het adres staan fouten;
- er is gebruik gemaakt van een vreemd handschrift of een slecht getypt adres (eventueel met spellingsfouten);

- sterk overdreven frankering: er staan té veel postzegels op de brief;
- het pakket is specifiek naar een bepaalde persoon gericht;
- de melding “persoonlijk” of “vertrouwelijk” bevindt zich op de omslag;
- ongebruikelijke wijze van bezorging;
- gebruik van vreemd materiaal zoals koorden, tapeband;
- er zijn elektrische/metalen draden zichtbaar, er is gebruik gemaakt van aluminiumpapier, en/of er bevinden zich gaten in de enveloppe (eventueel veroorzaakt door de metalen draden);
- de brief laat een vreemde geur achter;
- er zijn eventueel zachte “tik tak”- geluiden hoorbaar.

In het geval van een *dreigbrief*:

- dreigbrieven moeten met de nodige ernst behandeld worden. Wanneer iemand in contact komt met zo'n brief is het aangeraden hem dadelijk in een plastieken omhulsel of kartonnen briefomslag te steken. Er moet immers vermeden worden dat de brief door veel personen wordt gemanipuleerd. Dit bemoeilijkt het DNA-onderzoek dat de wetenschappelijke politie op het bewijsmateriaal kan uitvoeren.
- de ontvanger beslist best om de lokale politie op de hoogte te stellen van de dreigbrief, die conform de interne procedures van de geïntegreerde politie de gespecialiseerde diensten zal verwittigen.

1.11 Andere NBCR-incidenten¹

Wanneer een voorwerp een verdachte geur bevat of rook verspreidt, kan er mogelijk een link gelegd worden met verdachte poeders en sprays. Dit kan zich uiten wanneer bv. personeel of dieren (bv. waakhonden) plots ademhalingsproblemen krijgen, beginnen te braken of gedesoriënteerd zijn.

¹ METROPOLITAN POLICE, *Business Response to Terrorism*, London, Anti Terrorist Branch Counter Terrorism Section New Scotland Yard, s.d., 3-4.

In het geval van een NBCR–incident *buiten* het gebouw:

- alle airconditioning, computers, printers, fotokopieermachines en verwarmingstoestellen uitzetten alvorens het gebouw te verlaten voor evacuatie;
- alle vensters en deuren sluiten wanneer de kamer verlaten wordt. Het is aangeraden de sleutel nog op de deur te laten;
- verlaat het gebouw en begeef je zo ver mogelijk van de plaats van het incident;
- bij twijfel verlaat het gebouw niet direct, tot uitdrukkelijke toestemming van de hulpverleningsdiensten;
- blijf zo ver mogelijk uit de buurt van het voorwerp. Let op de windrichting, en ga met de wind in de rug staan, kijkend naar de plaats van het incident;
- verwittig de hulpdiensten.



In het geval van een NBCR–incident *binnen* het gebouw:

- wanneer het item nog intact is, het niet schudden of openen. Wanneer je het item reeds vastgenomen hebt, of het zich nog in je handen bevindt, plaats je het best in een transparante plastic tas, of container. Wanneer er geen container ter beschikking is, bedek je het voorwerp best met een voorwerp dat binnen handbereik is, bijvoorbeeld kleding, papier, ... en verwijder of verplaats je dit omhulsel niet;
- raak geen verdacht voorwerp aan, en verplaats het item niet naar een andere plaats;

- zet alle airconditioning, fotokopieermachines, printers, computers en verwarmingstoestellen uit;
- sluit alle deuren en vensters maar laat de sleutel in de kamer, evacueer de kamer;
- plaats indien mogelijk een zichtbare waarschuwing op de deur;
- begeef je naar een geïsoleerde kamer en vermijd in elk geval andere mensen indien mogelijk. Dit is onder andere noodzakelijk wanneer de verpakking mogelijk giftig is of een inhoud bevat die een besmettelijke ziekte zou kunnen voortbrengen;
- wrijf niet in de ogen, raak je gezicht niet aan en vermijd zeker lichamelijk contact met anderen;
- verwittig de hulpdiensten.

1.12 Geheime documenten¹

Speciale documenten, opnames, foto's, die na verloop van tijd niet meer nodig zijn, worden best onmiddellijk vernietigd, in kluizen opgeslagen of in ruimtes bewaard die enkel toegankelijk zijn voor personen met een veiligheidsmachtiging.

2 (Bouw)technische maatregelen

Aansluitend op de organisatorische maatregelen zijn ondersteunende (bouw)technische voorzieningen noodzakelijk om een degelijk niveau van beveiliging te realiseren.

Met (bouw)technische maatregelen wordt bedoeld alle veiligheidsmaatregelen die onmiddellijk met het gebouw te maken hebben. Voorbeelden zijn slagwerende beglazing, hekwerken, veiligheidsverlichting, mechanische beveiliging van ramen, deuren, garagepoorten, loskades en hang- en sluitwerk. Indien het mogelijk is, dient men met deze voorzieningen rekening te houden vanaf de planfase bij nieuwbouw. De kosten liggen opmerkelijk lager dan wanneer ze moeten aangebracht worden na

de oplevering van het gebouw. Naast de organisatie en inrichting van het gebouw, wordt er bij de (bouw)technische maatregelen ook aandacht besteed aan de onmiddellijke omgeving en de buitenkant van de onderneming, de aanleg van het terrein, de inplanting van en de toegang tot het gebouw, het gebruik van gepaste verlichtingen en afsluitingen.

(Bouw)technische maatregelen uiteten zich ook in de materiaalkeuze, de organisatie, de structuur van het gebouw en de mechanische - en bouwfysische beveiliging. In de hiernavolgende tips beperken we ons tot suggesties rond deuren en verlichting.²

2.1 Deuren³

Alle toegangsdeuren moeten voldoende stevig zijn en kunnen vb voorzien zijn van speciale sloten. Glazen deuren verdienen de nodige aandacht: ze bieden enerzijds als voordeel dat het bedrijf gemakkelijker verdachte situaties kan opmerken door hun transparantie, maar anderzijds is glas niet de veiligste en stevigste grondstof voor een deur.

Bij explosies wordt vaak veel schade veroorzaakt door rondslingerend glas van ramen en deuren. Een oplossing is om te kiezen voor beglazing met een anti-splinterfilm en tevens de dikte van het glas aan te passen aan de plaatsen waar het risico voor terroristische dreigingen het hoogst is.

2.2 Verlichting⁴

- Het belang van een goede veiligheidsverlichting mag niet onderschat worden. Een potentiële terrorist wil ongestoord en onopgemerkt zijn gang gaan. Tijdsgebrek en de kans op ontdekking dwingen hem om de klus zo snel mogelijk te klaren. Een goede verlichting schrikt af en is tevens essentieel voor een goede kwaliteit bij het filmen van de camera.

¹ OVERSEAS SECURITY ADVISORY COUNCIL (OSAC), *Guidelines for protecting U.S. Business Information Overseas*, s.l., United States Department of State, 1994, 9.

² FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 41, 43, 57.

³ HOME OFFICE, *Bombs: Protecting People and Property: a handbook for managers*, s.l., Home Office, s.d., 11-12.

⁴ *Ibid.*, 11.

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 60.

- Veiligheidsverlichting in combinatie met andere fysieke barrières en een snelle alarmopvolging, kan de terrorist van zijn plannen doen afzien.
- Een goede permanente verlichting op de parking werkt ontmoedigend. Het gaat hier om verlichting die indringers duidelijk zichtbaar maakt. Permanente nachtverlichting kan met een schemerschakelaar of een tijds klok automatisch worden ontstoken en gedoofd.
- Een “schrikverlichting” biedt als ontegensprekelijk voordeel dat via een bewegingsmelder een felle lamp zal aanspringen. Dit zal zowel onze eigen aandacht trekken, maar eveneens een afschrikkend effect hebben op de indringer, vooral als er in de omgeving toezicht is.

3 Elektronische maatregelen¹

Elektronische maatregelen zijn complementair en kunnen niet los gezien worden van de organisatorische en bouwtechnische maatregelen.

De effectiviteit van deze maatregelen hangt af van de manier hoe er mee wordt omgegaan. Zo wordt de preventieve waarde van een camera niet optimaal benut wanneer de beelden niet “live” op een monitor worden bekeken. Evenzeer is een duur elektronisch alarmsysteem zinloos, wanneer niemand weet hoe er op de juiste manier mee moet omgegaan worden. Bovendien is in de beveiligingsbranche de technologische vernieuwing quasi niet te volgen. Dit is een zware last voor de verantwoordelijke van het systeem omdat hij zich op de hoogte moet houden van de recentste ontwikkelingen. Daarenboven is elektronica storingsgevoelig. Een goed onderhoud van onder meer de alarmsystemen, camera- en videobewaking is dus een noodzaak voor de effectiviteit van deze middelen.

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 41, 43.
HOME OFFICE, *o.c.*, 11.

3.1 Alarminstallatie^{1 2}

Er bestaan verschillende soorten alarmen. Welk soort alarm gekozen wordt, moet grondig in relatie gebracht worden met de accommodatie van het gebouw en de omstandigheden. Een buitensirene is een geluidstoestel dat hoorbaar is buiten het beveiligde goed. Een alarmsysteem met buitensysteem moet ook voorzien zijn van een buitenlicht waarvan lichtsignalen zichtbaar zijn vanaf de openbare weg. Het buitenlicht functioneert tot het alarm is uitgeschakeld.

Een alarmsysteem is een complexe installatie. Een deugdelijk alarmsysteem is op maat samengesteld. De aard van het te beveiligen gebouw, de activiteiten die plaats vinden in de onderneming en de gewoonten van de gebruiker spelen hierbij een rol.

3.2 Camerasystemen^{3 4}

Camera's zijn van groot belang voor de interne en externe veiligheid van het bedrijf. Als ze goed geplaatst zijn, kunnen ze een bijdrage leveren aan de preventie van terrorisme. Door hun aanwezigheid kunnen de terroristen ook gefilmd worden, dit vergemakkelijkt indien nodig in een latere fase het identificeren van daders of van getuigen. *Camerabewaking* zorgt voor een registratie in "real time" via een monitor. De beelden worden naar een controlepost gestuurd, waar de monitors worden bekeken en de camera's kunnen worden bijgesteld. Wanneer men over *videobewaking* spreekt worden de beelden opgeslagen op een videoband. Voor het optimaal functioneren van cameratoezicht is vooral een kwalitatief hoogstaande installatie en plaatsing noodzakelijk. Niet alleen de technische kwaliteiten van de componenten zijn bepalend voor het uiteindelijke resultaat, ook de manier waarop de apparatuur is geïnstalleerd is heel belangrijk. Mindere of slechte resultaten zijn te wijten aan factoren zoals:

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 69-70.

² Opgelet : plaatsing en gebruik van alarmsystemen is aan een bijzondere regelgeving onderworpen : zie <http://www.vigilis.be>

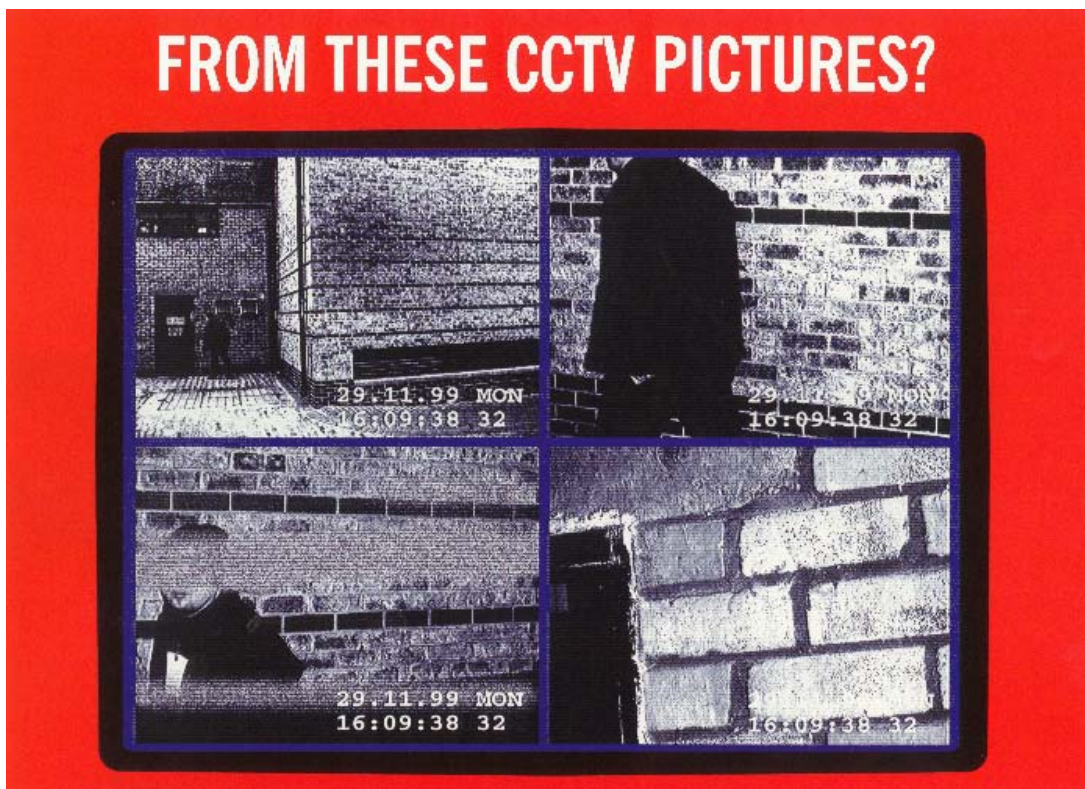
³ HOME OFFICE, *o.c.*, 11.

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 73-75.

METROPOLITAN POLICE, *Could you identify this criminal from these CCTV pictures?*, London, Metropolitan Police, s.d.

⁴ Opgelet ! Rekening dient te worden gehouden met de regels inzake de bescherming van de persoonlijke levenssfeer Zie : <http://www.privacy.fgov.be>

- een gebrek aan voorlichting over de mogelijkheden van camerasystemen;
- een gebrek aan een duidelijke doelstelling vooraf wat betreft de installatie van de camera;
- een onevenredige aandacht voor de techniek in plaats van de functionaliteit;
- het ontbreken van een opnametest;
- een gebrek aan goede gebruikersinstructies;
- een gebrek aan onderhoud van de apparatuur;
- het ontbreken van een degelijk bandenmanagement. Er moet aandacht besteed worden aan het regelmatig vervangen van de videobanden. Immers, wanneer camera's niet goed onderhouden worden, leveren ze slecht (en dus onbruikbaar) beeldmateriaal op;
- de videotapes worden na het filmen best nog minimum één maand bewaard;
- de tijd en de display moeten correct geïnstalleerd worden;
- een goede kwaliteit van videobanden moet worden gebruikt;
- de camera's moeten goed geplaatst zijn, zodat mensen en voertuigen duidelijk kunnen gefilmd worden;
- nepcamera's worden door de meeste criminelen snel herkend.



4 ICT-maatregelen¹

4.1 Algemene preventieve ICT-aanbevelingen

Computers kunnen voor enorme veiligheidsproblemen zorgen. Ze bevatten grote massa's aan informatie. Wanneer computersystemen onbeveiligd zijn, kan de terrorist gemakkelijk aan informatie geraken of productieprocessen negatief beïnvloeden. Cybercriminaliteit heeft tot doel computersystemen, telecommunicatienetwerken of kritische infrastructuur zoals controle – of financiële systemen aan te vallen.

Sinds de opkomst van het internet is het voor terroristen mogelijk om wereldwijd te opereren. Door de verspreiding van virussen kunnen ze ervoor zorgen dat computersystemen en –bestanden een grote schade oplopen. Het is tevens mogelijk om op deze manier geïnformatiseerde (productie)processen stil te leggen. Verder kunnen terroristen via hacking aan bepaalde nuttige informatie geraken. Via de verspreiding van virussen in bepaalde mails kunnen ze ervoor zorgen dat ze aan de nodige emailadressen of cruciale gegevens kunnen geraken. Computers die in netwerk staan kunnen gemakkelijk en snel geïnfecteerd worden.

Via cyberterrorisme kan de informatietechnologie dus op drie manieren getroffen worden:

- op een directe manier tegen het informaticasysteem zelf, bijvoorbeeld door hacking;
- op een fysieke manier, tegen kritische ICT-infrastructuur;
- via een vertrouwde persoon of door het binnenglippen in de onderneming, teneinde dan toegang tot het systeem verkrijgen.

Om zich te beschermen tegen mogelijke vormen van cyberterrorisme, zijn meerdere beveiligingsmaatregelen mogelijk.

Om virussen te weren moet er eerst nagedacht worden dat de software, diskettes en CD's van betrouwbare bronnen komen. Wanneer de software afkomstig is van buitenuit, is het noodzakelijk ze te laten scannen door een anti-virusprogramma dat up to date gehouden is, zodat eventuele virussen tijdig kunnen worden gedetecteerd.

¹ NCPC, *United for a Stronger America: Citizens Preparedness Guide*, s.l., USA Freedom Corps Department of Justice, s.d., 84.

OVERSEAS SECURITY ADVISORY COUNCIL (OSAC), *Guidelines for protecting U.S. Business Information Overseas*, s.l., United States Department of State, 1994, 2.

FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, o.c., 51.

Computers moeten beveiligd zijn met de nodige paswoorden. Telkens een personeelslid vertrekt, al is het maar voor enkele minuten, dient hij uit te loggen. Werknemers moeten alert zijn wanneer ze verdachte e-mail ontvangen, of e-mail van onbekende personen.

Computers worden best bewaard achter gesloten deuren en laptops in een kluis. Laptops in het bijzonder moeten altijd goed in het oog gehouden worden. Op luchthavens kunnen draagbare PC's vaak tijdelijk ontvreemd worden om bepaalde gegevens te kunnen overzetten op een andere computer. Dit is een mogelijke handeling om aan bepaalde informatie of gegevens te geraken.

Tenslotte is het zinvol om van belangrijke computerbestanden dagelijks een kopie te maken, die op een andere plaats bewaard wordt. Als computergegevens dan worden gestolen, gaat het werk tenminste niet verloren. Deze kopie wordt bij voorkeur niet mee naar huis genomen.

4.2 Concrete preventieve ICT-aanbevelingen¹

- Installeer recente antivirusprogramma's en actualiseer ze regelmatig;
- installeer "firewall"-toepassingen om hackers buiten te houden;
- maak regelmatig backups van programma's en gegevens en bewaar ze op een veilige plaats;
- stel een algemeen document op met richtlijnen voor normaal gebruik van de ITC-systemen;
- stel een richtlijn op inzake veiligheidsvoorschriften bij ITC-gebruik;
- aan alle werknemers zou duidelijk moeten gemaakt worden dat zij ook een rol spelen in de beveiliging van bedrijfsgegevens in het algemeen en van de ICT-infrastructuur in het bijzonder;
- de naleving van het ICT-gebruiksbeleid moet gecontroleerd ;
- er wordt best een ICT-beveiligingsverantwoordelijke aangeduid;
- bedrijfskritische ICT-systemen worden best, indien mogelijk, weg van het internet gehouden;

¹ L. BEIRENS, *Algemene aanbevelingen voor een veiliger ICT-gebruik*, Brussel, FCCU, 2001, 1.

- de systeemklok van de server moet regelmatig met de atoomklok op internet gesynchroniseerd worden;
- activeer log-toepassingen op firewall, proxy-servers en netwerktoegangen.

4.3 Aanbevelingen voor slachtoffers van ICT-criminaliteit¹

- Verbreek de verbinding met externe systemen zoals het internet;
- noteer volgende gegevens:
 - laatst bezochte websites / schuilnaam van chatpartner / Internetadres (IP) van correspondent
 - exact tijdstip van het ogenblik van de feiten (indien mogelijk tot op de seconde);
- evalueer: is de schade belangrijker dan het herstarten van de ICT-verbindingen?
 - indien het *herstarten* het belangrijkste is: maak dan een volledige backup vooraleer het systeem te herinstalleren
 - indien de *schade* het belangrijkste is: blijf overal af en verwittig politiediensten;
- bewaar alle logbestanden in hun originele vorm;
- wissel geen e-mails uit over uw eigen ICT-systeem omtrent het incident;
- wijzig alle paswoorden en indien mogelijk de namen van de gebruikers;
- check op het internet de gekende beveiligingsproblemen voor je besturingssysteem;
- breng de beschikbare beveiligingsupgrades aan in je besturingssysteem;
- herstel enkel de internetverbinding indien je zeker bent dat alle beveiligingsgaten gedicht zijn.

¹ Ibid., 1.

5 Personele beveiliging

De inzet van het personeel vormt het sluitstuk van de beveiliging. Om tot een integraal beveiligingsplan te komen – zeker in bedrijven met een complexe (personeels)structuur – is er meer nodig dan een reeks technische voorzieningen. De personele maatregelen worden daarom beschouwd als aanvulling op (bouw)technische en elektronische maatregelen. Vaak is de werking van de effectiviteit van deze middelen afhankelijk van de inzet en kennis van het personeel omtrent het (correct) gebruik ervan. Daarnaast vormt het personeel in vele gevallen de basis voor de organisatorische maatregelen. Hiermee wordt bedoeld: welke afspraken er gemaakt zijn betreffende de verantwoordelijkheden, hoe wordt er gereageerd op problemen, ... Kortom, welke zijn de bestaande afspraken en regels voor het personeel.¹

Grote bedrijven doen vaak beroep op een *externe beveiligingsfirma*. Kleinere bedrijven kunnen ook door het personeel zo verspreid mogelijk tewerk te stellen, zorgen voor een goed overzicht op het bedrijfsterrein. In sommige gevallen kan het nuttig zijn om enkele waakhonden in te schakelen. Bedrijven kunnen ook samen een overeenkomst sluiten met hun “buur”-bedrijven die op hetzelfde industrieterrein gevestigd zijn, om een externe beveiligingsfirma te laten surveilleren.

¹ FEDERALE OVERHEIDSDIENST BINNENLANDSE ZAKEN, *o.c.*, 41.

Conclusie

De bedrijfswereld kan dus het slachtoffer worden van terroristische of extremistische acties. Hun kwetsbaarheid uit zich in het feit dat zij door terroristen of extremisten zowel als middel en/of als doel kunnen gezien worden. Een terroristische actie kan derhalve heel uiteenlopende gevolgen hebben. Daarom is het aangewezen dat bedrijven preventief optreden om dergelijke acties te proberen voorkomen of in elk geval de gevolgen ervan te beperken.

Om aan een degelijk preventiemanagement te doen, heeft de firma best een beeld van wat het terrorisme en het extremisme betekent en wat de actuele tendensen van deze fenomenen zijn. Wanneer deze stap volbracht is, kan de onderneming gebruik maken van een Business Continuityplan, wat het voordeel biedt dat het stelselmatig opgebouwd is.

Tot slot kunnen er aan de hand van een dreigings- en risicoanalyse bepaalde preventieve beveiligingsmaatregelen gehanteerd worden, die specifiek kunnen ingevuld worden volgens de noden en de verwachtingen van de onderneming.