

TIPS & IDEEËN VOOR BEDRIJFSBEVEILIGING BETER VOORKOMEN DAN GENEZEN!



Met de medewerking van:



VBO vzw

Ravensteinstraat 4
1000 Brussel
T + 32 2 515 08 11
F + 32 2 515 09 99
info@vbo-feb.be
www.vbo.be

Verantwoordelijke uitgever

Olivier Joris
Wolvenbergstraat 17
1180 Brussel

Publicatieverantwoordelijke

Stefan Maes

Redactie

Federale Gerechtelijke Politie
Christine Darville-Finet (Verbond van Belgische Ondernemingen)
Gilbert Geudens (Commissie Bedrijfsbeveiliging van het VBO)

Vormgeving en pre-press

Vanessa Solymosi, Landmarks

Druk

Geers Offset

Wettelijk depot: D/0140/2010/11

Cette brochure est également disponible en français.
Een gedrukte versie van deze uitgave kunt u bestellen bij Paola Bulot,
Dienst Mailing & Secretariaat, pb@vbo-feb.be, fax 02 515 09 55.

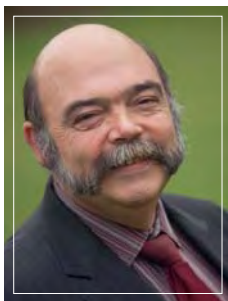
De inhoud van deze brochure vindt u eveneens op www.vbo.be
(publicaties > gratis brochures)

TIPS & IDEEËN VOOR BEDRIJFSBEVEILIGING

BETER VOORKOMEN DAN GENEZEN!



Christine Darville-Finet
Hoofd van het Juridisch
departement van het VBO



Gilbert Geudens
Voorzitter van de commissie
Bedrijfsbeveiliging van het VBO



Paul Van Thielen
Directeur-generaal van de
Federale Gerechtelijke Politie

Criminaliteit is een fenomeen waar Belgische ondernemingen niet aan ontsnappen. Het is enigszins begrijpelijk dat niet alle bedrijven voldoende of de nodige aandacht besteden aan dit probleem. Het nemen van beveiligingsmaatregelen draagt niet rechtstreeks bij tot de realisatie van de commerciële doelstellingen. Men mag echter niet uit het oog verliezen dat het verwaarlozen van criminele risico's belangrijke schade kan toebrengen aan het bedrijf.

Het is in deze context dat het Verbond van Belgische Ondernemingen (VBO) – in samenwerking met de Federale Gerechtelijke Politie – een brochure heeft opgesteld om u te sensibiliseren naar preventie toe. De bedoeling is niet om alle fenomenen in detail te overlopen, maar wel om uw aandacht te vestigen op bepaalde modi operandi en het nemen van preventiemaatregelen hieromtrent.

Niet alle onderdelen in een bedrijf zijn even kwetsbaar, maar het spreekt voor zich dat plaatsen waar met geld wordt gewerkt, waar waardevolle goederen worden gestockeerd of waar men gevoelige informatie bewaart, bijzondere aandacht verdienen!

Het is altijd beter om te voorkomen dan te genezen.

Uit de politionele statistieken merkt men dat de beveiligingsmaatregelen die door bepaalde sectoren werden genomen, lonen. De inbraken in bedrijven en handelszaken zijn dalend voor het vierde jaar op rij. Het aantal pogingen stijgt, wat aantoonde dat de crimineel het moeilijker heeft om binnen te geraken.

De diefstallen met geweld, en in het bijzonder gewapenderhand – die een zeer traumatiserend effect hebben op de slachtoffers –, tonen een licht stijgende trend. De diefstallen gewapenderhand tonen een verschuiving van klassieke, maar intussen goed beveiligde doelwitten (zoals banken, postkantoren, geldtransporten) naar minder beveiligde en meer kwetsbare sectoren (kleine winkels, benzinestations, horecasector, boekhandels, nightshops, apothekers, enz.).

Bij de cijfers die in de brochure vermeld zijn, is het belangrijk rekening te houden met het 'dark number' of de incidenten die niet geregistreerd werden bij de politie en dus niet voorkomen in de statistieken. Hiermee willen we uw aandacht trekken op het feit dat alle aangiften van groot belang zijn. Het is enkel als de politie alle stukken van de puzzel heeft, dat de dadergroep in kaart kan worden

gebracht en er tegen kan opgetreden worden. Hiermee willen we u aanmoedigen om systematisch klacht in te dienen. Voor sommige delicten kan het simpelweg online.

De oprichting van het Permanent Overlegplatform Bedrijfsbeveiliging (in uitvoering van het Federaal Veiligheids- en Detentieplan¹) heeft tot doel de private sector en de overheid dichter bij elkaar te brengen. Naast de federale stuurgroep (die een meer coördinerende functie waarneemt), werden vier werkgroepen opgericht die initiatieven uitwerken rond specifieke thema's (informaticacriminaliteit, bescherming van het wetenschappelijk en economisch potentieel, terrorisme, beeldvorming en georganiseerde criminaliteit). Het belang van deze publiek-private samenwerking als één van de vele middelen in het geïntegreerde veiligheidsbeleid, werd ook opgenomen in de Kadernota Integrale Veiligheid van 30-31 maart 2004.²

Zie ook andere realisaties zoals de brochure 'Terrorisme en extremisme, welke maatregelen kunnen bedrijven nemen?'³ en de creatie van het early warning system⁴.

Deze informatiebrochure is één van de concrete resultaten van de werkzaamheden binnen de werkgroepen.

De brochure heeft geenszins de intentie een naslagwerk te willen zijn inzake bedrijfsbeveiliging. Naast een algemene sensibilisatie omtrent specifieke beveiligingsproblemen, wil deze brochure een aantal praktische tips en adviezen aanreiken (hoofdzakelijk van organisatorische aard) die kunnen bijdragen tot het opstarten of verbeteren van uw beveiligingsprocedures, om aldus een verhoogde beveiliging van en in uw bedrijf te bekomen. Kleine dingen maken soms grote verschillen! ●

¹ Ministerie van Justitie, 31 mei 2000 – project 25: <http://www.dekamer.be/FLVVB/pdf/50/0716/50K0716003.pdf>.

² <http://www.info-zone.be/wet/plp35/kanoplp35.pdf>.

³ www.vbo.be.

⁴ Zie p. 42 hieromtrent.

Inleiding

I. Fenomenen en criminele risico's	6
Bommeldingen en/of verdachte zendingen	6
Situering	6
Algemene preventieve maatregelen	7
Hoe reageren in geval van een incident?	7
Diefstal zonder braak	9
Situering	9
Preventieve maatregelen	10
Hoe te reageren in geval van een incident?	12
Ramkraken	12
Situering	12
Preventieve maatregelen	13
Hoe te reageren in geval van een incident?	14
Inbraak	14
Situering	14
Preventieve maatregelen	16
Hoe te reageren in geval van een incident?	17
Afpersing	17
Situering	17
Preventieve maatregelen	18
Hoe te reageren in geval van een incident?	18
Fraude	19
Situering	19
Preventieve maatregelen	20
Hoe te reageren in geval van een incident?	20
Misbruik van informatie	21
Situering	21
Preventieve maatregelen	21
Hoe te reageren in geval van een incident?	22
Rip deal	23
Situering	23
Preventieve maatregelen	24
Hoe te reageren in geval van een incident ?	25
Gijzeling	26
Situering	26
Preventieve maatregelen	26
Hoe te reageren in geval van een incident?	28

Diefstal gewapenderhand	29
Stuering	29
Preventieve maatregelen	30
Hoe te reageren in geval van een incident?	34
Carjacking	35
Stuering	35
Preventieve maatregelen	35
Hoe te reageren in geval van een incident?	36
Diefstal uit voertuigen	36
Stuering	36
Preventieve maatregelen	37
Hoe te reageren in geval van een incident?	38
Vandalisme	39
Stuering	39
Preventieve maatregelen	40
Hoe te reageren in geval van een incident?	41
2. Early warning system: een bedrijfsinformatienetwerk tegen terroristische dreigingen	42
Wat is het 'Early warning system'?	42
Voor en door wie?	43
Wat niet?	43
Hoe?	43
Publiek-private samenwerking	44
Werking van het informatieverkant	44
Voorbeelden van toepassingen van het informatieverkant en/of het contactpunt	45
3. Technopreventieve adviezen	48
Wat is technopreventie?	48
Wat is een technopreventief adviseur?	49
Wat is de rol van de technopreventief adviseur?	49
Hoe kom ik in contact met de dichtstbijzijnde technopreventief adviseur?	50
Camerabewaking	50
Andere beveiligingsmaatregelen	51
4. Nuttige links en websites	52
Police on web	52
eCops	53
Checkdoc	53
DOCSTOP	54
5. Bijlage	56



1 Fenomenen en criminele risico's

BOMMELDINGEN EN/OF VERDACHTE ZENDINGEN

Situering

Bommelding

Uit politionele informatie blijkt dat deze problematiek (met aanverwante fenomenen zoals poederbrieven en/of bompakketten) zich zeer frequent voordoet.

Vandaar het belang dat u er met enkele eenvoudige maatregelen kan voor zorgen dat een maximum aan informatie ter beschikking wordt gesteld van het bedrijf én de autoriteiten, zodat een eventuele risico-evaluatie mogelijk wordt en de

eventueel noodzakelijke maatregelen een maximum effect kunnen hebben.

Verdachte zendingen

Hoe kunt u een verdachte zending herkennen? Dit is helaas geen exacte wetenschap; het zal in functie van een aantal elementen zijn waardoor een zending als verdacht bestempeld kan worden. Enkele elementen kunnen zijn:

- vreemde vorm en/of ongebruikelijk gewicht;
- bij manipulatie indruk van inhoud andere dan papier;
- ongebruikelijke hoeveelheid kleefband werd gebruikt;

- land/stad van herkomst van de afzender van de briefwisseling stemt niet overeen met de poststempel;
- zendingen geadresseerd aan iemand die het bedrijf reeds verlaten heeft; incorrecte titel; alleen een titel of gericht aan een totaal onbekende persoon;
- vreemde geur;
- vreemde vlek(ken) of verkleuringen;
- aanwezigheid van poeder;
- zendingen zonder afzender;
- onverwachte brieven en/of van een totaal onbekende/onbruikelijke afzender;
- onleesbaar of oncontroleerbaar afzenderadres;
- de melding 'persoonlijk' of 'vertrouwelijk' op de omslag;
- handgeschreven of slecht getypt adres; grote spellingsfouten.

Algemene preventieve maatregelen

Voor bommeldingen, poederbrieven, bom-brieven en -pakketten en verdachte voertuigen kunnen volgende algemene preventieve maatregelen genomen worden:

- geef uw personeel een algemene briefing betreffende dit fenomeen;
- voorzie in personeelsleden die desgevallend de politiediensten kunnen bijstaan bij een sweeping (grondige controle van de gebouwen);
- voorzie in een grondplan per verdieping, in een verantwoordelijke per afdeling of verdieping, voor een eventuele evacuatie alsook in een aparte ontruimingsweg (top-down);

- stel een standaarddocument als geheugensteun ter beschikking van het personeel en bepaal een duidelijke communicatielijn (naar wie gaat deze informatie ASAP (As Soon As Possible) binnen het bedrijf).

Hoe reageren in geval van een incident?

Bommelding

- Doorloop het bovenvermelde standaarddocument.
- Stel onmiddellijk de beveiligingsverantwoordelijke op de hoogte.
- Beslis (directie), in samenspraak met de lokale politie, al dan niet tot een evacuatie.

Stel een standaarddocument als geheugensteun ter beschikking van het personeel en bepaal een duidelijke communicatielijn.

- Bij telefonische bommelding: zie checklist met vragen in bijlage.

Poederbrieven

Het systematisch laten behandelen van brieven in een afgesloten ruimte door een ervaren personeelslid verdient in dit kader uiteraard de voorkeur:

- Niet schudden, noch enige andere vorm van manipulatie; open de zending niet, ►►

- ▶▶ ook niet gedeeltelijk en vermijd ieder onnodig contact met de zending.
- Plaats het stuk apart, minimaal in één 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 het stuk kan manipuleren.
- Evacueer de ruimte en sluit ze af voor anderen.
- Vermijd ventilatie en leg de airconditioning stil.
- Indien poeder werd gemorst: kuis dit niet op, maar bedek het met een kleingstuk, papier, e.d. ter vermijding van verdere verspreiding.

Bij een verdachte zending, open de zending niet en vermijd ieder onnodig contact.

- 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.
- Verwittig uw beveiligingsverantwoordelijke, die een lijst zal opmaken ten behoeve van de autoriteiten van alle personen die vermoedelijk met de zending in contact zijn gekomen en die de lokale politie zal verwittigen.



Bombrief of -pakket

- Niet aanraken noch verplaatsen; memoiseren van zoveel mogelijk details.
- Rustig (trillingen vermijden) de plaats verlaten (eventuele aanwezige collega's meenemen).
- De plaats afsluiten (ervoor zorgen dat de plaats niet kan betreden worden door collega's).
- Geen gebruik van gsm of draagbare radio's.
- Omgeving (perimeter) laten 'bewaken' op afstand.
- Verwittig de veiligheidsverantwoordelijke onmiddellijk, die de lokale politie zal verwittigen.

Verdacht voertuig

Dezelfde reflexen als bij een bombrief of -pakket dienen in acht genomen te wor-



den. Een perimeter van 200 meter is echter aangewezen.

Uiteraard is de lokale politie uw gesprekspartner bij uitstek in geval van dergelijke incidenten. Zij zullen op hun beurt, indien nodig, via de geëigende kanalen de federale politie en/of andere instanties inlichten.

Een voorafgaand contact tussen de beveiligingsverantwoordelijke en/of ondernemer en een vertegenwoordiger van de lokale politie lijkt niet overbodig teneinde in geval van incidenten zo vlot mogelijk te kunnen werken en dit uiteraard in het belang van beide partijen.

DIEFSTAL ZONDER BRAAK

Situering

Veel bedrijven hebben reeds een diefstal gekend. Het is dan ook niet verwonderlijk dat bedrijven beschermingsmaatregelen nemen op het vlak van diefstalpreventie. Bij diefstal is er meestal sprake van ont-

vreemding van geld of goederen uit een gebouw. Het komt echter ook voor dat goederen uit bedrijfswagens worden gestolen. Bovendien moet u rekening houden met de mogelijkheid van diefstal van de bedrijfswagens zelf.

In veel gevallen wordt diefstal door externe daders gepleegd. Daarnaast blijkt dat ook een bepaald percentage ondernemingen het slachtoffer wordt van diefstal door eigen personeelsleden.

De kans op diefstal heeft uiteraard te maken met de aard van de artikelen die u heeft en de (mogelijke) aanwezigheid van kasgeld. Begunstigende factoren zijn:

- de aanwezigheid van potentiële daders (typische 'rondhangplekken' voor probleemjongeren of junks,...);
- de afwezigheid van 'sociale ogen' (passanten of bewoners in de buurt die informeel en vaak onbewust een oogje in het zeil houden of van bewakers en politie die formeel toezicht houden);



- ▶▶ • een ongunstige omgeving (aanwezigheid van hindernissen die de zichtbaarheid beperken);
- te gemakkelijke toegang(en) tot de bedrijfsgebouwen en de eventuele aanwezigheid van vluchtwegen (hoe meer in- en uitgangen hoe aantrekkelijker uw gebouw voor dieven).

Preventieve maatregelen

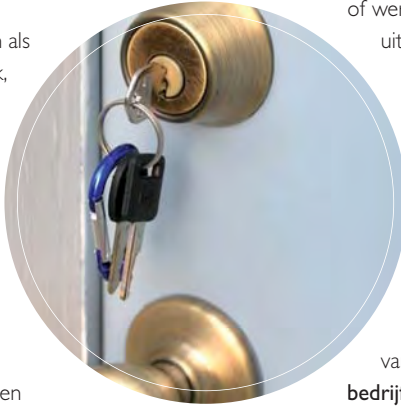
Er zijn veel maatregelen mogelijk waarmee u de kans op diefstal of de gevolgen van eventuele diefstal kunt verkleinen. Die maatregelen kunnen sterk van bedrijf tot bedrijf verschillen. Het principe berust op 3 aspecten: de organisatorische maatregelen, de mechanische (bouwkundige) maatregelen en de elektronische maatregelen. Meer uitleg hierover in punt 3: technopreventieve adviezen.

Er zijn veel maatregelen om de kans op diefstal te verkleinen.

- Beperk de mogelijke buit door geld op onregelmatige tijdstippen naar de bank te brengen, door grondstoffen niet eerder in te slaan dan u ze nodig heeft en door producten zo snel mogelijk af te leveren bij de klant.
 - Verminder het contante geldverkeer ten gunste van elektronisch betalingsverkeer.
 - Beperk de toegang tot 'gevoelige' ruimtes.
- Controleer de toegang tot uw bedrijfsruimtes. Sluit ruimtes af als het publiek daar niet hoeft te zijn.
 - Leg aantrekkelijke of waardevolle spullen buiten het bereik van potentiële daders.
 - Merk en registreer apparatuur en voorraad; neem een foto van waardevolle voorwerpen.⁵
 - Spreek met uw personeelsleden af in hoeverre zij kantoorartikelen en -apparaten voor privédoeleinden mogen gebruiken.
 - Laat bedrijfswagens niet onbeheerd achter op de openbare weg.
 - Zorg ervoor dat uw vrachtwagenchauffeurs direct na aankomst bij een afnemer hun goederen uitladen. Niet eerst eten of overnachten in een hotel. Houd daarmee rekening bij het samenstellen van uw rijschema.
 - Zorg voor een goed sleutelbeheer:
 - ontwikkel discipline rond wie de sleutel mag hebben van wat;
 - gebruik sleutels die niet na te maken zijn;
 - laat nooit sleutels op vitrines, kluisen of deuren zitten;
 - vervang sloten als de sleutel verloren of gestolen is;
 - verander regelmatig cijfercombinaties van kluisen. Doe dit zeker na het ontslag van een medewerker.

- Ken uw klanten. Observeer mensen en maak, wanneer iemand binnenkomt, direct contact. Leer ook uw personeel dat te doen.

- Wees alert op signalen als rondhangen in de zaak, non-koopgedrag, vragen die weinig steek houden, verdachte voertuigen, mensen die bijzondere aandacht hebben voor de beveiliging, verdachte geldwisselingen.



- Doe een beroep op een vergunde bewakingsonderneming of interne bewakingsdienst (wet van 10 april 1990 tot regeling van de bijzondere en private veiligheid⁵).
- Overweeg het inbouwen van plaatsbepalingsapparatuur (after-theft trackingsysteem) in uw bedrijfswagens waarmee de politie gestolen wagens snel kan opsporen.
- Specifiek voor winkeldiefstal vindt u meer informatie bij de vzw Preventie en Veiligheid (Mariannestraat 34, 1180 Brussel – 02 345 99 23).
- Organiseer regelmatig **uitgangsc controles** bij uw medewerkers. **Cao 89** regelt de

modaliteiten van de uitgangsc controles bij werknemers en definieert ze als volgt: “controles van werknemers die plaatsvinden wanneer zij de onderneming of werkplaats verlaten en die uitsluitend gericht zijn op het voorkomen of vaststellen van de ontvreemding van goederen in de onderneming of op de werkplaats”. U kan de gedetailleerde informatie terugvinden in de brochure van het VBO ‘**Maak uw bedrijf veiliger na uitgangsc controles**’⁷ (beschikbaar via www.vbo.be > publicaties).

De dienst Preventie van de FOD Binnenlandse Zaken heeft reeds verschillende brochures opgesteld met goede tips (‘manieren om uw beroepslokalen te beveiligen’, ‘veilig zelfstandig ondernemen’, ‘voorkom diefstal op uw werf’, ‘voorkom diefstal uit je auto’, etc.).⁸

Veel bedrijven investeren voornamelijk in technische beveiliging. Informatie m.b.t. **het plaatsen van camera's** in het raam van diefstalpreventie vindt u terug in punt 3, p. 50 van deze brochure. Andere – organisatorische – maatregelen zijn ook zeer belangrijk en mogen niet uit het oog verloren worden. ►►

⁵ Registratieformulier is beschikbaar in leaflet ‘Save your numbers’ op www.besafe.be.

⁶ Meer informatie vindt u op www.vigilis.be.

⁷ www.vbo.be.

⁸ Die brochures kan u consulteren en bestellen op www.besafe.be.

►► Hoe te reageren in geval van een incident?

Uiteraard is de lokale politie uw gesprekspartner bij uitstek in geval van dergelijke incidenten. Zij zullen op hun beurt, indien nodig, via de geëigende kanalen de federale politie en/of andere instanties inlichten. Winkeldiefstal kan ook online aangegeven worden op het virtuele loket van de politie via www.Police-on-web.be. Meer uitleg hieromtrent vindt u in punt 4 van deze brochure.

RAMKRAKEN

Situering

Het college van procureurs-generaal definieert een ramkraak als: "het plegen van een diefstal of poging tot diefstal door middel van braak op een etalage, deur of toegangspoort van een (zelfstandige) onderneming of handelszaak,

waarbij een voertuig, een voorwerp (dat al dan niet door een voertuig wordt voortgeduwd) of enig ander slagwapen wordt gebruikt en dit met de bedoeling de buit snel weg te nemen".

Feiten van diefstal met inklimming of valse sleutels vallen m.a.w. niet onder de definitie van ramkraken.

Voornamelijk worden uitstalramen van bedrijven waar goederen verkocht worden, gevisieerd, maar het kan evenwel ook een deur of een toegangspoort betreffen. In bepaalde gevallen dringt men binnen via een sectionale laadpoort, die gemakkelijker in te rijden is en/of het risico van kwetsuren verkleint.

Omwille van het hoge vermogen dat nodig is om op een snelle manier een slagkracht teweeg te brengen, is een voertuig het klassieke rammiddel. In bepaalde gevallen zullen de daders een voorwerp gebruiken om de aanwezige technopreventieve maat-



regelen te omzeilen, zoals het gebruiken van een fietsrek, een houten balk, een vuilnisbak als rammiddel... In functie van de situatie passen de daders hun modus operandi aan. Voorhamers (al dan niet met een boorkop erop gelast), betonblokken, riooldeksels blijken immers even effectief als rammiddel. Bovendien kunnen dergelijke zaken dikwijls in de omgeving van het bedrijf worden gevonden en vertoont de vluchtwagen aldus geen sporen van het misdrijf.

Veel van deze ondernemingen hebben een technopreventieve beveiliging, zoals alarm-systemen met doorverbinding naar een centrale van een bewakingsonderneming. De daders rekenen er evenwel op om in de tijdspanne van de doormelding aan de politie en de 'aanrijtijd' van de interventie hun slag te kunnen slaan.

Door de beveiliging van de handelszaken is de modus operandi dikwijls een combinatie van verschillende inbraakmethodes. Zo worden draad en hangsloten doorgeknipt met een kniptang, om het eventuele rolluik weg te rukken of omhoog te duwen en daarna met een voertuig achterwaarts de vitrine of inkomdeur in te beuken. De alarmsystemen worden dikwijls gesaboteerd door camera's omhoog te duwen of af te dekken, of door met isolatiemateriaal het alarmgeluid uit te schakelen. De goederen worden meestal in de winkel op een dekzeil gegooid en worden vervolgens in de kofferruimte van de vluchtauto gelegd. Het vluchtvoertuig wordt vaak in de onmiddellijke omgeving gestolen. Het binnendringen in de handelszaak, het stelen van

de buit en het wegvluchten gaan zeer snel: dikwijls binnen een paar minuten.

Meestal gebeurt er ook een voorverkenning door de daders enkele dagen voor de ramkraak.

Het aantal ramkraken vertoont de laatste jaren een duidelijk dalende trend.

Dankzij de veiligheidsmaatregelen die genomen werden, zijn de ramkraken minder en minder aantrekkelijk voor de dieven.

Dankzij de veiligheidsmaatregelen die genomen werden (plaatsen van betonpalen, bloembakken voor het uitstalraam, enz.) is deze modus operandi minder en minder aantrekkelijk voor de dieven.

Preventieve maatregelen

- Beperk zoveel mogelijk de hoeveelheid en/of de waarde van de tentoongestelde goederen in de winkel, gebruik indien mogelijk dummy's.
- Indien er één of meer bewakingscamera's in de winkel zijn:
 - stel op zijn minst één camera verdekt op, maar plaats ook een camera duidelijk in het zicht;
 - zorg dat de apparatuur van goede kwaliteit is;
 - kijk na of de gemaakte beelden duidelijk en bruikbaar zijn (vermijd tegenlicht);
 - zie ook hoofdstuk 3, p. 50 inzake de modaliteiten bij camerabewaking. ►►

- ▶ • Heb aandacht voor verdachte personen en voertuigen. Zeer vaak voeren de daders enkele uren tot enkele dagen voordien een verkenning uit. Zij hebben



oog voor de plaats waar de camera's opgesteld staan, maar ook voor de omvang van de mogelijke buit en de stevigheid van de toegangsdeuren. Noteer de nummerplaten van verdachte voertuigen en geef ze samen met een persoonsbeschrijving onmiddellijk door aan de lokale politie met het oog op een eventuele interceptie en controle.

- De aanwezigheid van 'sociale ogen' (passanten of bewoners in de buurt die informeel en vaak onbewust een oogje in het zeil houden).
- Vermijd dat in de omgeving van de winkel voorwerpen los liggen/staan die door

de daders gemakkelijk kunnen gebruikt worden om de etalage te rammen (afvalcontainers, fietsrekken,...).

- Probeer, indien mogelijk, een vlotte doorgang voor de daders in de winkel te vermijden (bijvoorbeeld door het opstellen van hindernissen). Snelheid tijdens de uitvoering van hun actie is immers hun grote troef.
- Laat weinig geld achter in de kassa. Laat indien mogelijk de kassa open. Zo wordt vermeden dat ze wordt meegenomen of beschadigd.

Hoe te reageren in geval van een incident?

Uiteraard is de lokale politie uw gesprekspartner bij uitstek in geval van dergelijke incidenten. Zij zullen op hun beurt, indien nodig, via de geëigende kanalen de federale politie en/of andere instanties inlichten. In afwachting van de vaststellingen en eventuele sporenopname door het gerechtelijk labo, dient u de 'plaats delict' zoveel mogelijk in de toestand te laten waarin het zich bevond (niet opruimen, zo weinig mogelijk aanraken, sporen beveiligen indien nodig).

INBRAAK

Situering

Veel ondernemingen hebben jaarlijks te maken met inbraak. Meestal is de buit aanzienlijk. Braakschade komt daar nog eens bij. Het is dan ook niet te verwon-

deren dat de meeste bedrijven beschermingsmaatregelen nemen om dit risico te verlagen.

Sommige sectoren zijn meer getroffen dan andere: de risicograad van de horecazaken en grootwarenhuizen ligt hoger dan voor andere bedrijven. De meest gestolen goederen in handelszaken en bedrijven zijn: geld, rookwaren, diefstal uit of van brandkast, computers, voeding en alcohol, communicatiemiddelen, kleding, enz.

Een inbraak gaat niet altijd gepaard met diefstal. Het is mogelijk dat een inbreker zich toegang tot uw bedrijf verschaft om warm te slapen, om vernielingen aan te richten, om brand te stichten of om (op een later tijdstip) een overval te plegen.

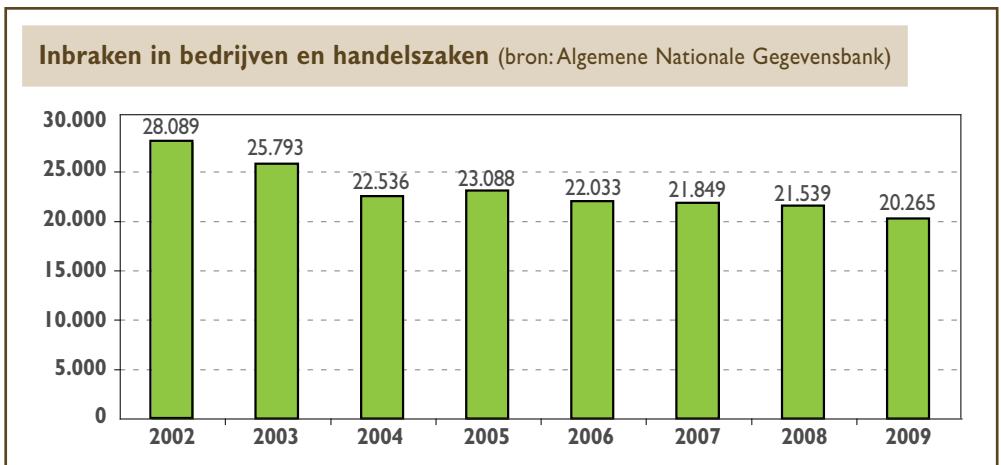
Welke preventiemaatregelen u ook treft, een inbreker kan ze altijd proberen te

omzeilen. Als hij maar genoeg tijd krijgt. Een goede beveiliging tegen inbraak stoelt daarom op twee principes. U moet een inbreker zo snel mogelijk detecteren en u moet ervoor zorgen dat een inbreker veel tijd nodig heeft om zijn doel te bereiken.

Detecteer een inbreker zo snel mogelijk en zorg ervoor dat hij veel tijd nodig heeft om zijn doel te bereiken.

Als u deze principes goed toepast, kunt u in een vroeg stadium van een inbraak alarm slaan. Daarmee wint u tijd om de nodige actie uit te voeren en de inbreker te doen aanhouden.

De cijfers van inbraken in handelszaken en bedrijven kennen al enkele jaren een daling. ►►



► • **Wanneer wordt er nu ingebroken in bedrijven en handelszaken?**

De meeste inbraken worden gepleegd tijdens de wintermaanden. De woensdag en de vrijdag zijn de 'populairste' dagen. Er wordt meestal 's nachts ingebroken tussen middernacht en 6 uur 's ochtends.

• **Wat zoeken de daders?**

Geld is het meest geëerd en verschijnt dan ook op de eerste plaats in de lijst van de gestolen goederen. Voedingswaren, brandkasten, communicatiemiddelen en multimedia vervulden de top 5 en vertegenwoordigen 80% van wat in bedrijven en handelszaken wordt gestolen.

Plaatsen waar met geld wordt gewerkt, of waar men gevoelige informatie bewaart, verdienen bijzondere aandacht.

Niet alle onderdelen in een bedrijf zijn even kwetsbaar, maar het spreekt voor zich dat plaatsen waar met geld wordt gewerkt, waar waardevolle goederen worden gestockeerd of waar men gevoelige informatie bewaart, bijzondere aandacht verdienen!

Preventieve maatregelen

Inbraakpreventie is gebaseerd op:

- het verhogen van de pakkans;
- het bemoeilijken van de toegang tot gebouwen;
- het beperken van de buit, verhandelbaarheid en de toegebrachte schade;
- de nauwkeurige aangifte bij diefstal.

Bij maatregelen tegen inbraak, moet u allereerst denken aan organisatorische maatregelen zoals:

- wees voortdurend bewust van het risico op inbraak. Zorg ook dat uw personeel dat ook is;
- let op het goed afsluiten van ramen en deuren. Sluit ook tussendeuren af. Laat de sleutels van (tussen)deuren niet op voor de hand liggende plaatsen achter. Zorg dat er niet meer sleutels in omloop zijn dan strikt noodzakelijk;
- merk en registreer uw goederen en apparaten. Neem foto's van waardevolle voorwerpen⁹;
- maak dagelijks een kopie van uw computerbestanden en bewaar die in een kluis elders. Als uw computers worden gestolen of vernield, gaat er niet meer dan één dag werk verloren. Neem de kopie niet mee naar huis;
- organiseer een controleronde voor de sluiting van de onderneming zodat niemand zich laat insluiten;
- zorg voor een goede alarmopvolging. Een goede inbraakbeveiliging heeft immers alleen zin als u snel nadat een inbreker is gesignaleerd de juiste actie in gang zet.

Nadat de organisatie van uw beveiliging goed is, kunnen technische (bouwkundige en elektronische) maatregelen effect hebben:

- zorg ervoor dat u al bij de toegang van uw bedrijfsterrein een onderscheid kunt maken tussen een indringer en een toevallige voorbijganger (toegangscontrole);
- zorg voor terreinverlichting en elektronische detectiesystemen;



Zo kunt u bijvoorbeeld op een bedrijfsterrein met de andere ondernemers gezamenlijk afspraken maken voor permanente surveillance door een bewakingsonderneming.¹⁰

Hoe te reageren in geval van een incident?

Uiteraard is de lokale politie uw gesprekspartner bij uitstek in geval van dergelijke incidenten. Zij zullen op hun beurt, indien nodig, via de geëigende kanalen de federale politie en/of andere instanties inlichten. Het is dan ook aangewezen om steeds aangifte te doen, bij de lokale politie, in geval van een inbraak.

- let op de gevel- en dakbeveiliging: inbraakwerende ramen, deuren, dakramen en lichtkoepels, goed hang- en sluitwerk, elektronisch alarm, rolluiken;
- plaats betonnen plantenbakken en/of paaltjes op strategische plaatsen zodat een magazijningang niet met een auto vernield kan worden;
- interne beveiliging met afgesloten deuren, eventueel met elektronisch alarm. Compartimentering: plaats de meest waardevolle spullen in de best afgesloten ruimte. Doe geld, waardepapieren en vertrouwelijke stukken in een kluis;
- sociale waakzaamheid.

Een andere beveiligingsmethode betreft de inzet van een bewakingsonderneming.

In afwachting van de vaststellingen en eventuele sporenonopname door het gerechtelijk labo, dient u de 'plaats delict' zoveel mogelijk in de toestand te laten waarin het zich bevond (niet opruimen, zo weinig mogelijk aanraken, sporen beveiligen indien nodig).

AFPERSING

Situering

Met afpersen wordt bedoeld: iemand onder bedreiging dwingen iets te geven. Er moet een oorzakelijk verband zijn tussen het gebruik van geweld of de bedreiging en de afgifte van de afgeperste zaak. ►►

⁹ Het registratieformulier is beschikbaar in leaflet 'Save your numbers' op www.besafe.be.

¹⁰ Voor informatie, zie <http://www.vigilis.be> en <http://www.apeg-bvbo.be>.

- ▶ Afpersing kan zich manifesteren onder verschillende verschijningsvormen:
 - racketeering;
 - productafpersing;
 - chantage.

Racketeering is een bijzondere vorm van afpersing, waarbij de daders die deel uitmaken van een bende, één of meer zelfstandigen de geregelde betaling van sommen geld onder bedreiging afdwingen. In ruil daarvoor krijgt de handelaar 'bescherming' of kan hij zijn commerciële activiteiten voortzetten zonder verdere 'ongemakken'.

Productafpersing onderscheidt zich van andere afpersingsvormen door het feit dat een bedrijf wordt afgeperst door te dreigen producten te contamineren of te saboteren.

Chantage kan omschreven worden als het zich doen overhandigen van een handtekening, geld, of waarden onder bedreiging van compromitterende onthullingen die de goede naam van personen of het bedrijf kunnen schaden.

De afpersers kunnen het slachtoffer persoonlijk ontmoeten, of via telefoon, brief of andere middelen contacteren. Het gebeurt ook dat afpersers contact nemen met een derde partij, zoals de pers, politie, een over-

heidsdienst, verdeelcentra..., om hun eisen mee te delen.

Samen met informaticacriminaliteit ervaart de bedrijfswereld deze criminaliteit als een reële dreiging.

Preventieve maatregelen

Tegen afpersing kan men weinig preventieve maatregelen nemen. Wel kan een bedrijf zich voorbereiden op

'hoe te reageren' wanneer men het slachtoffer wordt van een afpersing. Dit maakt het mogelijk om op een flexibele wijze en met kennis te handelen.

Het is aangewezen dat een bedrijf beschikt over een crisismanagementplan, waarin onder meer de analyse van de mogelijke incidenten, de interne informatiestroom, de verwittigingsprocedures, de beslissingsprocedures en eerste reacties zijn opgenomen.

Hoe te reageren in geval van een incident?

Bij de aanpak van de crisis is de vrijwaring van de fysieke integriteit van de bedreigde persoon de eerste prioriteit van alle betrokkenen.

Om te vermijden dat sporen worden beschadigd of gewist, is het aangewezen de dreigbrief bij ontvangst minimaal te manipuleren, digi-



taal te fotograferen en vervolgens onmiddellijk in een papieren omslag te plaatsen. Vervolgens kan dan voortgewerkt worden met een kopij van de dreigbrief (digitale foto).

Bij telefonische afpersing; zie checklist met vragen in bijlage.

Bij een afpersing wordt een klacht ingediend bij de federale gerechtelijke politie van het arrondissement¹¹, die een onderzoek zal voeren met bijzondere aandacht voor discretie, om de commerciële belangen van het bedrijf niet te schaden.

FRAUDE

Situering

Fraude is een containerbegrip. Er bestaat geen uniforme definitie van het begrip 'fraude' en evenmin een eenduidige onderverdeling ervan. Drie fraudetypes kunnen onderscheiden worden:

- interne fraude: de fraudeur is werknemer **binnen** het bedrijf;
- externe fraude: de fraudeur bevindt zich **buiten** het bedrijf;
- bedrijfsfraude: het bedrijf is **zelf** fraudeur.

Het is quasi onmogelijk een juist criminaliteitsbeeld te schetsen van fraude, omdat het dark number groot is. Daardoor weten we dat bedrijven het probleem onderschatten. Nochtans zijn er regelmatig signalen dat

binnen een bedrijf wordt gefraudeerd. Zulke signalen zijn bijvoorbeeld: een afwijkend declaratiepatroon, een afwijkend verlofpatroon (het niet of nauwelijks opnemen van vakantiedagen), een afwijkend werkpatroon (het als eerste binnenkomen en als laatste het bedrijf verlaten), het ontbreken van meerdere offertes bij belangrijke inkoop, veel handgeschreven bonnen, veel correcties op kastickets, veelvuldig gebruik van creditnota's, regelmatig verkopen van beschadigde goederen, het ophalen of afleveren van goederen op ongebruikelijke tijdstippen, een sollicitant heeft een te mooi cv of uitsluitend kopieën van diploma's. De schade die bedrijven lijden als gevolg van fraude is aanzienlijk. De meeste schade wordt veroorzaakt door fraude met kostendeclaraties, verduistering van financiële middelen en diefstal van goederen. Volgende factoren creëren of beïnvloeden de gelegenheid tot fraude:

- te groot vertrouwen vanwege de werkgever;
- zwakke interne controle;
- interne controle die omzeild wordt;
- het ontbreken van ethische normen;
- het ontbreken van procedures of de procedures niet correct toepassen;
- beïnvloeding door andere collega's;
- gebrekkig antecedentenonderzoek bij indiensttreding;
- lacunes in het automatiseringssysteem.

Vaak wordt de zaak intern opgelost, in veel gevallen middels de hulp van privédetectives. ►►

¹¹ De adressen kunt u vinden op <http://www.info-zone.be>.

►► Preventieve maatregelen

Bij fraudepreventie kunnen drie stappen ondernomen worden.

Een **eerste stap** bij fraudepreventie is '**management-awareness**'. Veel bedrijfsleiders zitten verlegen met deze vorm van criminaliteit omdat het vaak gaat over eigen personeelsleden. Antifraudemaatregelen kunnen de werksfeer bederven en een klimaat van wantrouwen scheppen op de werkvloer.

Fraude komt echter in de beste bedrijven voor. Daarom bestaat de **tweede stap** erin om het probleem binnen de onderneming **bespreekbaar** te maken. Door het fraude-risico bij het personeel aan te kaarten, maakt men de per bedrijf geldende specifieke normen waaraan zich te houden duidelijk (gedragslijn inzake declaraties, relatiegeschenken, gereedschap en bedrijfsapparatuur; air-miles,...). Speel open kaart met werknemers inzake periodieke controles en het waarom ervan.

Door het frauderisico bij het personeel aan te kaarten, maakt men de per bedrijf geldende specifieke normen waaraan zich te houden duidelijk.

Als **derde stap** wijst de praktijk uit dat bijna de helft van de fraudegevallen kon voorkomen worden mits een degelijke **interne controle**. Er bestaat echter geen algemene regel voor preventieve acties ter bestrijding

van fraude, omdat de verschijningsvorm ervan telkens anders is (zie supra omtrent definitie). Fraude heeft immers doorgaans geen repetitief, noch recurrent karakter. Hierna volgen enkele tips.

- Leg de uitvoering van werkzaamheden en de controle erop bij verschillende personeelsleden.
- Controleer inkoop, voorraadbeheer en verkoop. Breng cijfers met elkaar in verband en ga afwijkingen na.
- Ga de betrouwbaarheid van afnemers en leveranciers na. Zorg voor beveiliging van computerbestanden. Houd er rekening mee dat uw systeembeheerder onbeperkt toegang heeft tot al uw gegevensbestanden.
- Ga, wanneer u iemand in dienst neemt, zijn of haar referenties na.
- Beperk de bevoegdheid van stagiaires en uitzendkrachten en zorg dat zij goed begeleid worden.

Hoe te reageren in geval van een incident?

Indien een fraudeprobleem zich binnen de onderneming stelt, dient rekening gehouden te worden met de opsporingswet. Opsporingen mogen enkel gebeuren door vergunde privédetectives¹². De aanpak van fraude door de private sector kan o.w.v. zijn finaliteit, snelheid en middelen verschillen van de aanpak vanuit de publieke sector.

Ook hier is de lokale politie het officiële aanspreekpunt voor meldingen.

MISBRUIK VAN INFORMATIE

Situering

Geen onderneming kan bestaan zonder informatie: strategische informatie, informatie over productieprocessen, bedrijfsadministratie,...

Informatie is doorgaans op drie manieren aanwezig in het bedrijf: op papieren drager; opslag in computerbestanden of in het hoofd van medewerkers.

Steeds vaker spelen computerbestanden een centrale rol in de opslag en verwerking van informatie. Dat maakt uw onderneming extra kwetsbaar omdat de informatie via elektronische weg gestolen, gemanipuleerd en geblokkeerd kan worden. Dikwijls zonder dat de ondernemer het zelf merkt. De schade is vaak onherstelbaar:

Ook informatie op papier en in het hoofd van medewerkers is kwetsbaar. Papieren kunnen gestolen en vervalst worden. Mensen kunnen loslippig zijn of gedwongen worden bepaalde informatie prijs te geven.

Preventieve maatregelen

Bij beveiliging van informatie gelden drie uitgangspunten: vertrouwelijke informatie



moet vertrouwelijk blijven, betrouwbare informatie moet betrouwbaar blijven, beschikbare informatie moet beschikbaar zijn.

U kunt de volgende maatregelen treffen:

- geef het verschil tussen vertrouwelijke en niet-vertrouwelijke informatie duidelijk aan. Zorg dat uw personeel op de hoogte is van het vertrouwelijke karakter van sommige informatie. Zorg dat vertrouwelijke informatie alleen bekend is bij ►►

¹²Wet van 19 juli 1991 tot regeling van het beroep van privédetective, www.vigilis.be.

- ▶▶ personeelsleden die ermee moeten werken. Laat geen vertrouwelijke stukken op bureaus, naast de kopiërenmachine of aan de kopieermachine rondslingeren;
- beveilig uw systeem tegen inbraak via internet of het WIFI-netwerk, onder meer door gebruik van een firewall. Laat alle binnenkomende transmissies scannen door een antivirusscanner. Wanneer u vreemde diskettes, cd-roms of USB-dragers inleest, controleer deze dan vooraf op de aanwezigheid van virussen;
- beveilig uw computers tegen onbevoegd gebruik. Regel de toegangscontrole tot (onderdelen van) uw computernetwerk via goede wachtwoorden of meer performante systemen zoals digipass of e-ID. Bepaal duidelijk wie er bevoegd is om gegevens in te zien, toe te voegen en/of te veranderen. Laat de wachtwoorden regelmatig veranderen;
- maak dagelijks een back-up van uw computerbestand en dit zowel van de programmatuur als van de gebruikersgegevens (databanken);
- sensibiliseer nieuwe medewerkers, uitzendkrachten en stagiaires om zorgvuldig met computerprogramma's en -bestanden om te gaan;
- gebruik geen illegaal verkregen software;
- crypteer indien nodig vertrouwelijke gegevens op USB-sticks;
- maak afspraken met uw personeel over geheimhouding en zet die afspraken op papier. Herinner uw personeel aan deze afspraken wanneer het dienstverband eindigt.

Hoe te reageren in geval van een incident?

De neiging bestaat om deze inbreuken intern af te handelen. Toch is het aangeraden **steeds** aangifte te doen bij de lokale politie omwille van het strafrechtelijke karakter van de inbreuk.

Bewaar in dit geval de informaticasystemen zoveel mogelijk in hun oorspronkelijke toestand. Ga zelf geen opsporingen doen in het systeem.



RIP DEAL

Situering

Al een paar jaar wordt een fenomeen in België waargenomen en opgevolgd, nl. de 'RIP DEAL' (komt van het Engels 'to rip': scheuren – deal: transactie). Dit fenomeen is begin jaren 90 ontstaan en trof eerst het zuiden van Europa en het UK. In België wordt de RIP DEAL niet als zodanig in het strafwetboek vermeld, maar de feiten kunnen gekwalificeerd of verenigd worden onder de volgende benamingen: oplichting, valsmunterij, gewone diefstal, diefstal met geweld, vereniging van misdadigers, criminele organisatie, witwassen.

Uit de analyse van de modus operandi blijkt duidelijk een economische en financiële oplichting.

Deze zou als volgt gedefinieerd kunnen worden: wisseloplichting of diefstal met internationale omvang, gepleegd onder de dekking van een roerende of onroerende transactie op een som geld of een waarde, met of zonder geweld, door een gestructureerde criminele groep.

De **kenmerken** van de RIP DEAL:

- de daders zien een advertentie in de pers of op het internet meestal voor de verkoop van een onroerend goed, maar ook soms van juwelen, een boot, paarden,... om de aandacht van de potentiële verkoper te trekken dankzij de aangekondigde geloofwaardigheid;
- de daders handelen stapsgewijs en het doel is het vertrouwen van de slachtoffers te winnen:
 - door zich voor te stellen als valse experts, juristen en notarissen, valse Arabische sjeik, enz.;
 - door een aantrekkelijke offerte, een handel in contant geld op de hele transactie voor te stellen, of door het goed te onderschatten, met het oog op wissel in contant geld ten voordele van de verkoper voor wat het praktische wisselpercentage betreft en met het voorwendsel van een voordelige lokale fiscaliteit;

De 'RIP DEAL' is een economische en financiële oplichting.

- de onderhandelingen gaan snel in de richting van een wisselkwestie of transactie in contant geld;
- een eerste transactie vindt plaats met winst om het slachtoffer te verleiden en met het oog op een tweede transactie die leidt tot de eigenlijke RIP DEAL en tegelijk tot de diefstal van een grote som contant geld (duizenden euro's);
- met kunstgrepen (afspraken in luxehotels, dure voertuigen, smaakvolle kledij), daar het doel is in valse vennootschappen te laten geloven;
- door het gebruik van verschillende identiteiten bij elke stap;
- door afspraken te maken meestal in een ander land dan het thuisland van de slachtoffers;



- ▶▶ - door de slachtoffers aan te zetten hen andere potentiële slachtoffers voor te stellen door ze te doen geloven dat ze hun nadeel kunnen terugkrijgen;
- geldwaardenuitwisseling.
Eigenlijk ontvangt het slachtoffer reproducties van biljetten met, onder de papieren ring rond de bundel, facsimile inschrijvingen, nl. Walt Disney – ristorante italiano of pretpark. Maar dit zijn geen valse biljetten.
De uitwisselingen gebeuren met :
 - euro tegen facsimile van 1.000 Zwitserse frankbiljetten;
 - euro tegen facsimile van 200 eurobiljetten;
 - euro tegen valse euro;
 - \$ en Canadese dollars tegen valse euro;
 - euro tegen valse lening- of investeringscontracten;



- ze gebruiken niet systematisch geweld, maar kunnen wel geweld gebruiken indien de transactie of de uitwisseling te lang duurt. Meestal rukken ze de koffer vol met geld uit de handen van het slachtoffer;
- meeste benadeelden komen uit volgende landen: Italië, Zwitserland,

Duitsland, Luxemburg, België, Spanje, Frankrijk, UK. Ze komen van alle sociale lagen en worden gekozen volgens hun financiële toestand. Het doel is het politieke en gerechtelijke optreden te beperken.

Opmerking: het spreekt vanzelf dat de daders schuldig zijn, en niet de slachtoffers die geen klacht (durven) indienen uit angst voor fiscale controle. Sommigen hebben trouwens te goeder trouw perfect wettelijke en aangegeven bedragen in de transactie gestoken en verloren. De tactiek bestaat in feite in een manoeuvre van de daders, die hun aansprakelijkheid weerleggen door ze af te schuiven op de goedgelovige slachtoffers die werden gelokt met een niet aangegeven winst;

- het bedrag van het nadeel kan op honderden duizenden euro's geschat worden. De schatting is gedeeltelijk als wij de niet gemelde feiten en de verschillende kwalificaties in rekening nemen.

Preventieve maatregelen

Het publiek toelaten een beter zicht op het fenomeen te krijgen, zal alle potentiële slachtoffers aanzetten zeer wantrouwig te zijn.

De preventie ter zake kan in twee stappen.

- **Bewustmaking d.m.v. informatie**

Het grote publiek kan slechts bewust worden van de risico's, vooral inzake oplichting (gezien de verschillende modi operandi),

als het correcte informatie krijgt. Indien wij een preventieve impact wensen, is het opportuun deze informatie in de media regelmatig te verspreiden: radio; tv; vakpers (Test Aankoop, banken,...); internet.

De gereguleerde beroepen (make-lars, notarissen...) die contact kunnen heb-



Het bedrag van het nadeel van een 'RIP DEAL' kan soms op honderden duizenden euro's geschat worden.

ben met daders moeten ook gesensibiliseerd worden door ze te vragen:

- alle gekende nuttige inlichtingen zo snel mogelijk mee te delen aan de politiediensten;
- hun klanten te informeren en ze aan te zetten klacht in te dienen of alle nuttige inlichtingen te verschaffen;
- verdachte handelingen die mogelijks betrekking hebben op witwassen, door te melden aan de CFI (Celler Verwerking van Financiële Informatie¹³).

- **Partnerschap**

Het spreekt vanzelf dat de hierboven voziene maatregelen slechts uitgevoerd kunnen worden mits een partnerschap voor informatie-uitwisseling tussen de

gespecialiseerde politiediensten en de betrokken externe partners (vastgoedmakelaars, notarissen,...).

Hoe te reageren in geval van een incident?

- Geen vertrouwen hebben in alle aankoopvoorstellen via internet gevolgd door het sturen van e-mails van zogenaamde vastgoedmakelaars in het buitenland en handelend voor buitenlandse investeerders.
- Aandacht schenken aan het feit dat de kopers/daders de prijs niet onderhandelen.
- Geen voorstel tot transactie of uitwisseling in cash onder te voordelige voorwaarden aanvaarden. ►►

¹³ www.CTIF-CFI.be.

- ▶▶ • Elke afspraak in het buitenland, ofwel om een transactie te bespreken, ofwel om deze transactie uit te voeren, weigeren.
- Geen weerstand bieden bij gewelddaad zoals het uittrekken van de koffer.
- Bij twijfels of verdenking, de politiediensten verwittigen.
- Indien de RIP DEAL voltooid is, klacht indienen bij de politiediensten waar het feit plaatsgevonden heeft en in het thuisland van het slachtoffer.

GIJZELING

Situering

Gijzeling is "de aanhouding, de gevangenhouding of de ontvoering van personen om deze borg te doen staan voor de voldoening aan een bevel of een voorwaarde".

De ontvoering (kidnapping) van een kapitaalkrachtige persoon, met het oog op de uitbetaling van een losgeld, is een specifieke vorm van gijzeling.

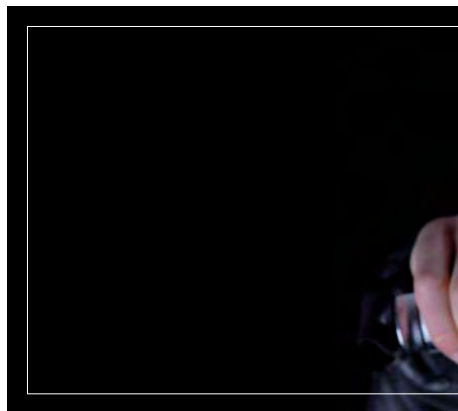
De daders van een gewapende overval, die verrast worden door de komst van de politie en personen gijzelen om de vlucht van de daders te verzekeren, is een voorbeeld van een niet-voorbereide gijzeling.

Een bijzondere vorm van gijzeling is 'tiger kidnapping': het gaat om de aanhouding, gevangenhouding of ontvoering van één

of meerdere personen, met het doel een werknemer of gemandateerde, een verwant of elk ander persoon te dwingen onmiddellijk waardepapieren, aanzienlijke geldsommen of eender welke vorm van losgeld, toebehorend aan een instelling of onderneming aan de daders te bezorgen. Vooral de banksector wordt met dergelijke zware misdrijven geconfronteerd.

Preventieve maatregelen

- Zorg voor sensibilisatie van uw kaderleden.
- Een bedrijf kan zich voorbereiden op 'hoe te reageren' wanneer een lid of leden van het bedrijf het slachtoffer wordt (worden) van een gijzeling. Zorg onder meer voor het opstellen en up-to-date houden van een vertrouwelijke steekkaart van kaderleden met gegevens zoals gezondheidstoestand, noodzakelijke medicijnen, betrokkenheid bij bepaalde



conflictsituaties, samenstelling gezin en contactgegevens...

- Het is aangewezen dat een bedrijf beschikt over een crisismanagementplan, waarin onder meer de analyse van de mogelijke incidenten, de interne informatiestroom, de verwittigingsprocedures, de beslissingsprocedures en eerste reacties zijn opgenomen.
- Potentiële slachtoffers van een gijzeling kunnen preventief een aantal beveiligingsmaatregelen treffen in de woning, op het werk en bij de verplaatsingen van en naar het werk. In het raam van zendingen naar het buitenland is het aanbevolen om een goede evaluatie van de plaatselijke toestand te maken, zoals:
 - lokaal criminaliteitsbeeld;
 - belangrijke gebeurtenissen die een mogelijke impact hebben op de openbare orde en veiligheid (verkiezingen, sociale conflicten, aanslagen,...);

- kennis omtrent mogelijke risicozones;
- dreigingsniveau inzake terrorisme;
- kwaliteit, betrouwbaarheid van lokale politiediensten;
- het politieke klimaat en de mogelijke repercussies voor het bedrijf.

Potentiële slachtoffers van een gijzeling kunnen preventief een aantal beveiligingsmaatregelen treffen in de woning, op het werk, enz.

Op basis daarvan kan een plan worden voorbereid: briefing kaderlid, aanduiding van veilige plaatsen, uitbouwen van een lokaal netwerk van contacten (consulaat, bepaalde ngo's,...) waar men terecht kan in geval van dreiging/nood.

- Men kan overwegen om zich te verzekeren tegen het risico van ontvoering.

Voor tiger kidnapping gelden volgende specifieke raadgevingen:

- wijzig sommige levenspatronen (verander eens van reisweg, reisuur, winkelgewoonten, parkeergewoonten);
- wees alert voor ongewone zaken. Verwittig bijvoorbeeld onmiddellijk de telefoonmaatschappij als je telefoon in panne valt of gestoord is. Heel belangrijk is ook dat je ongewone zaken of verdachte handelingen zo snel en zo gedetailleerd mogelijk meldt. Zo kan de politie proactief en gericht patrouilles uitvoeren;
- in de wagen: kijk wat meer in je achteruitkijkspiegel zodat je het merkt als iemand ►►



- ▶▶ je verdacht lang volgt. Neem nooit een onbekende mee in je wagen. Zorg ervoor dat je weet waar het politiekantoor of een andere veilige plaats zich bevindt langs de reiswegen;
- let wat meer op voertuigen in de buurt van je woning. Bijvoorbeeld: woon je op het platteland en zie je twee dagen na elkaar een onbekende wagen: noteer de nummerplaat en verwittig de politie en je buurtinformatienetwerk als er één bestaat;

Meld zo snel en zo gedetailleerd mogelijk ongewone zaken of verdachte handelingen.

- vraag aan de preventieadviseur van de lokale politie om langs te komen en ga na hoe je je beter kan beveiligen (bv. geen sleutel onder een bloempot leggen of oprit en deuringangen verlichten, een alarminstallatie of alarmknop plaatsen);
- laat je agenda niet rondslingeren. Bespreek je agenda wel met je naaste medewerkers zodat iemand goed op de hoogte is van je plannen en afspraken;
- installeer een alarmknop en beperk het aantal mensen dat toegang heeft tot de kluis.

Hoe te reageren in geval van een incident?

Bij de aanpak van de crisis is de vrijwaring van de fysieke integriteit van de gegijzelden de eerste prioriteit. Belangrijk is

het inwinnen van informatie over de gegijzelden en de daders.

Bij een ontvoering wordt onmiddellijk contact opgenomen met de politie via het noodnummer 101 of 112. Het onderzoek zal gevoerd worden met bijzondere aandacht voor discretie, om de commerciële belangen van het bedrijf niet te schaden. Het is aangewezen de discretie te bewaren wanneer de gijzeling nog niet bekend is bij het publiek.

Alle mogelijke sporen die wijzen naar de gijzeling en de daders worden gevrijwaard, opdat de politie de nodige vaststellingen kan verrichten.

De omgeving (familie of een verantwoordelijke van het bedrijf) kan volgende stappen ondernemen:

- in chronologische volgorde nota nemen van alle feiten zoals ze zich hebben voorgedaan;
- een codewoord afspreken voor herkenning bij de volgende oproepen;
- een bewijs vragen van de bewering dat 'x' in hun 'bezit' is;
- pogen om een goede verstandhouding te bekomen;
- altijd benadrukken dat u niet de beslissende bent (indien bedrijf betrokken is);
- behandel niet zelf de brieven of andere mededelingen die betrekking hebben op de eisen en berg deze onmiddellijk op in een papieren omslag.

Enkele raadgevingen voor het slachtoffer:

- uw bevrijdingskansen worden sterk beïnvloed door uw houding: goede

fysieke conditie, zelfdiscipline, geduld, zelfvertrouwen;

- naarmate de tijd verstrijkt, verhogen uw bevrijdingskansen;
- probeer zoveel mogelijk zaken te memo-riseren; houd uw geest bezig;
- weet dat men al het mogelijke zal doen om u te helpen, doch dit vraagt tijd.

DIEFSTAL GEWAPENDERHAND

Situering

Overvallen (of diefstallen gewapenderhand) komen minder frequent voor dan gewone diefstal en inbraak, maar de impact en traumatische gevolgen zijn des te groter. Vele bedrijven nemen maatregelen om zich te beschermen tegen dit probleem.

De diefstallen met geweld, en in het bijzonder gewapenderhand – die een zeer

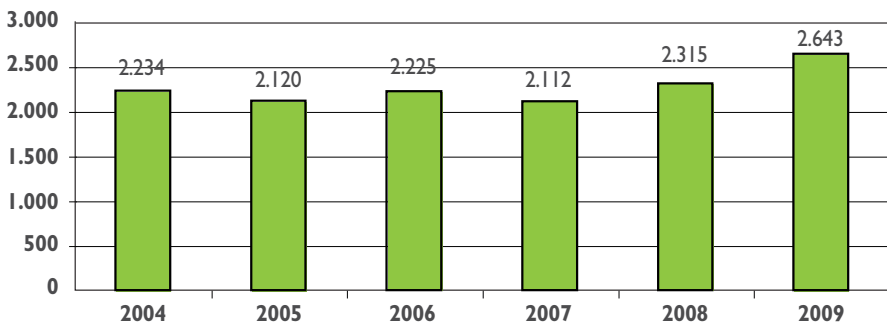
traumatiserend effect hebben op de slachtoffers –, tonen een licht stijgende trend.

De diefstallen gewapenderhand tonen een verschuiving van klassieke, maar intussen goed beveiligde doelwitten (zoals banken, postkantoren, geldtransporten) naar minder beveiligde en meer kwetsbare sectoren (zoals kleine winkels, benzinstations, horecasector; boekhandels, nightshops, apothekers, enz.).

Een overval vertoont volgende karakteristieken:

- een overval duurt meestal niet langer dan enkele minuten;
- in sommige gevallen zijn de daders niet gemaskerd;
- de meeste overvallers zijn uit op geld. Ze richten zich op de kassa. Waardepapieren en goederen zijn minder interessant;
- jonge onervaren overvallers kiezen het liefst makkelijke doelwitten uit zoals een snackbar of een winkel in hun eigen stad ►►

Evolutie diefstal gewapenderhand (excl. op de openbare weg, car- en homejacking) - bron: DB DJB/DGH



- ▶▶ of buurt. Zij raken snel in paniek wanneer er tijdens de overval iets onverwachts gebeurt, waardoor de kans op geweld toeneemt;



© Federale politie / Communicatie dienst

- meer ervaren overvallers bereiden hun overval goed voor; werken in georganiseerd teamverband en hebben vooraf de vluchtweg al uitgestippeld. Zij zoeken doelwitten waar veel geld te halen is zoals banken, grote winkels, postkantoren, geldtransporten en juweliers;
- soms doen overvallers zich voor als klanten. Op een geschikt moment bedreigen zij het personeel en dwingen zij hen de kassa te openen.

Preventieve maatregelen

Het is belangrijk maatregelen te treffen om de kans op een overval te verkleinen. Wanneer u personeel in dienst heeft, bent u

bovendien, volgens de wet van 4 augustus 1996 betreffende het welzijn van de werknemers bij de uitvoering van hun werk en het koninklijk besluit van 17 mei 2007 betreffende de voorkoming van psychosociale belasting veroorzaakt door het werk, waaronder geweld, pesterijen en ongewenst seksueel gedrag op het werk, verplicht om maatregelen te treffen om uw personeel te beschermen tegen geweld en agressie op de werkplek, dus ook tegen overvallen. Het gaat daarbij zowel om materiële als organisatorische maatregelen om geweld op het werk te voorkomen.

Organisatie van de onderneming

- Organisatiecultuur en -structuur gericht op preventie.
- Zichtbare steun en betrokkenheid van de bedrijfsleiding om een oplossingsgerichte bedrijfscultuur mogelijk te maken.
- Preventiestructuur met preventieadviseur en vertrouwensperso(ou)w(en).
- Verbetering van de intermenselijke verhoudingen, samenwerkingsbevordering (teamwork, sociale steun en appreciatie zijn de beste remedie tegen geweld, pesterijen en ongewenst seksueel gedrag op het werk).
- Werken in duo voor 'gevaarlijke' functies of voor werknemers die zich bedreigd voelen.
- Inspraakmogelijkheden, laat medewerkers ook mee oplossingen voorstellen.
- Inbouw van meetbare indicatoren (vinger aan de pols houden) en organisatie van evaluatie en effectmetingen.
- Aandacht voor de problematiek van geweld, pesterijen en ongewenst seksueel

gedrag op het werk bij het onthaal van nieuwe werknemers of uitzendkrachten.

- Toewijzen van een peter of meter aan nieuwe werknemers of uitzendkrachten.
- Regelmatige rondgang in alle werkruimtes en kantoren door chef, preventieadviseur;...
- Grote hoeveelheden geld in kassa's (niet alleen in winkels) vermijden en het behandelen van geld verrichten uit het zicht van iedereen in een afgeschermd lokaal.
- Werkprogramma steeds doorgeven aan een collega (uren van afspraken, adressen, telefoonnummers,...) voor werknemers die in externe dienst werken.
- Risicoanalyse na feiten uitvoeren en hieruit bijkomende of aangepaste maatregelen afleiden (zie 'Organisatie van de onderneming' en 'Materiële inrichting van de arbeidsplaatsen').
- Samenwerking met lokale autoriteiten en naburige ondernemingen in geografische zones die vaak het doelwit zijn van of zich lenen tot externe agressie en geweld.

Materiële inrichting van de arbeidsplaatsen

- Gescheiden toiletten en kledkamers voor mannen en vrouwen.
- Geen snijdende of scherpe voorwerpen (brievenopener, schaar, cutter...) laten rondslingeren en voorwerpen die als projectiel zouden kunnen dienen, vastmaken.
- Hoeveelheid meubelen in de lokalen beperken.
- Aanpassing of (her)inrichting van de werkplaatsen indien blijkt dat deze niet adequaat ingericht zijn om een antwoord te bieden op (externe) agressie. Het kan gaan om (elektronische of

andere aanpassingen) om de risico's op geweld maximaal aan banden te leggen.

- Installatie van receptieruimtes, loketten, lokalen voor klantendiensten op plaatsen die goed zichtbaar zijn voor de andere werknemers en voor het publiek (het is bijgevolg aangewezen niet te veel affiches aan te brengen op de vensters opdat men er doorheen zou kunnen kijken).
- Toegangscontrole (toegangssas, drukknopsysteem,...).
- Schikking van het meubilair zodanig dat het de werknemer niet hindert in zijn bewegingsvrijheid en dat hij zich dichterbij de uitgang bevindt dan de klant.
- Gebruik van bredere en hogere tafels (bureaus, toonbanken) dan het gemiddelde om zoveel mogelijk fysisch contact te vermijden.
- Systemen van video- en radiobewaking.
- Alarm- en waarschuwingknop, automatisch geprogrammeerd noodnummer (interne bewaking, politie,...).
- Voldoende verlichting rond het gebouw en de ingangen.

Voor 'gevaarlijke' functies of voor werknemers die zich bedreigd voelen, is het aan te raden in duo te werken.

- Wachtruimtes moeten kalm en uitnodigend zijn: comfortabele zitplaatsen, **geen verblindende verlichting**, voldoende ruimte tussen de verschillende zitplaatsen en de tafel, meubilair verankerd in de grond, tijdschriften om wachttijden te ►►

- ▶▶ doden, afwezigheid van voorwerpen waarmee zou kunnen gegooid worden of die als wapens zouden kunnen dienen.

Voorlichting en opleiding van de werknemers

- Werknemers informeren over de risico's, de verschillende hulpmiddelen, preventie maatregelen en procedures (via de preventieadviseur; interne publicaties, gerichte folder; het intranet,...).

Gerichte trainingen kunnen een onderdeel zijn van het preventiebeleid.

- Een jaarlijkse sensibilisatiecampagne (video, getuigenissen, affiches, opleidingen,...).
- Affichering via informatieborden.
- Aandacht voor de problematiek van geweld en agressie bij het onthaal van nieuwe werknemers of uitzendkrachten.
- Werknemers moeten vaak over vaardigheden beschikken die ze tijdens hun opleiding niet hebben aangeleerd. Gerichte trainingen kunnen daarom een onderdeel zijn van het preventiebeleid (bv. vorming in communicatie, weerbaarheidscurcussen voor het omgaan met moeilijke klanten of assertiviteitstraining in het algemeen).

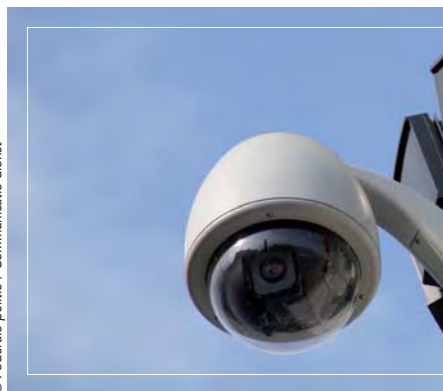
Volgende preventieve maatregelen kunnen genomen worden:

- let vooral op de risicomomenten en risicopunten:

- het openen en afsluiten van het bedrijf of de onderneming;
- de kassa;
- de plaats waar geld, waardepapieren of waardevolle goederen worden opgeborgen (zoals kluis);
- het intern waardetransport; telling van de ontvangsten en kasopmaak;
- het extern waardetransport of de zaakvoerder die het geld meeneemt naar huis;

- zorg voor een **overzichtelijke inrichting** in en rondom uw bedrijf:
 - zet strategische punten zo dat men zicht heeft op de ingang en het geheel;
 - zorg voor een goede verlichting in de werkplaats en bij de ingangen (zonder schaduwvlekken);
 - belemmer het zicht niet door de plaatsing van panelen;
 - houd de deuren naar achterliggende vertrekken steeds gesloten;
 - vraag bijkomend advies over interne

© Federale politie / Communicatie dienst



- veiligheid aan een technopreventief adviseur;
- laat via pictogrammen aan iedereen (dus ook aan potentiële overvallers) duidelijk weten dat de zaak goed beveiligd is;
 - verstandig **openen en sluiten**:
 - kijk uit naar verdachte personen, voertuigen of situaties;
 - indien mogelijk, open en sluit steeds met 2 personen;
 - controleer of niemand in de inrichting achterblijft en of bepaalde ingangen niet zijn klaargemaakt om te kunnen binnendringen;
 - sluit steeds stipt;
 - wees opmerkzaam voor sporen van braak;
 - wees gezond argwanend tegenover nieuw personeel van leveranciers of transporteurs;
 - laat bij sluiting de lege kassalade open;
 - controleer de toiletten alvorens af te sluiten (sluitingsronde);
 - doordacht omgaan met geld:
 - houd nooit meer geld in de kassa dan het noodzakelijke wisselgeld;
 - vermijd dat de kassa onnodig openstaat;
 - stimuleer het gebruik van elektronische betaalmiddelen;
 - installeer een afroomkluis met tijdsmechanisme en afficheer dit duidelijk;
 - tel het geld niet in het zicht van klanten;
 - beheer en transport van geld zijn een bedrijfsgeheim;
 - monteer een scherm boven de kassalade tegen 'kassagrijpen';
 - vermijd grote geldvolumes in uw kassa en berg grote ontvangsten bij voorkeur tussentijds op in een kluis of 'verberg' ze alvast op een andere veilige plaats;
 - geef met duidelijke opschriften aan dat er alleen kleingeld in de kassa is en dat klanten met grotere biljetten niet terecht kunnen aan de kassa;
 - vermijd bij waardetransporten vaste patronen. Ga het liefst overdag naar de bank. Als u gebruik maakt van een nachtkluis, let er dan op dat er niet met de kluis geknoeid is. Als de sleutel niet soepel in het slot past, breek de storting dan onmiddellijk af. Voer belangrijke transporten bij voorkeur met twee personen uit;
 - maak een goed sleutelplan. Beperk het aantal sleutels dat in omloop is. Bewaar omwille van overvalrisico's de kluis sleutel op een vaste plaats, maar laat hem nooit op de kluis zitten;
 - sensibiliseer ook het personeel voor alle beveiligingsaspecten.



►► Hoe te reageren in geval van een incident?

Mocht er zich een overval voordoen, pas dan het **RAAK**-principe toe.

- **Rustig:** probeer kalm te blijven. Maak geen onverwachte bewegingen. Tracht te vermijden dat de dader kan schrikken omdat iemand kan binnenkomen.
- **Aanvaarden situatie:** volg bevelen op en vermijd provocaties. Ga ervan uit dat het wapen echt is! Werk mee met de overvaller en ga niet in discussie. Bevestig door uw houding dat de overvaller de macht en de controle heeft.
- **Afgeven geld:** denk bij een overval niet (meer) aan uw bezittingen, maar denk aan de fysieke veiligheid van uzelf, uw personeel en uw klanten. Informeer daarom uw personeel van tevoren hoe in zo'n situatie te handelen. Licht de dader in over de kluisprocedure, c.q. het tijdslot.

- **Kijken:** probeer het signalement van de overvaller te onthouden, alsook de vluchtrichting en het vervoermiddel van de overvaller(s). Belemmer in geen geval de vluchtweg en probeer evenmin de overvaller te volgen. Overweeg de toepassing van een stil alarmsysteem om de politie te verwittigen.

Men moet tijdens een overval proberen **zelfcontrole** te behouden en **positief te denken**: "ik moet rustig blijven, hij komt niet voor mij, ik ga dit overleven!"

Met het oog op eventuele identificatie en aanhouding van de daders, hierbij enkele elementen en tips die het werk van de politie kunnen vergemakkelijken:

- fysieke details van de daders (lengte en omvang, taal en manier van spreken, schoenen of kledijonderdelen);
- kenmerken van vluchtwagen, eventueel nummerplaat en vluchtrichting;
- welke zaken heeft de dader aangeraakt;
- getuigen verzamelen;



- de zaak direct afsluiten en geen sporen uitwissen;
- signalement van de dader en details van de gebeurtenis onmiddellijk en individueel noteren;
- het verlies en de buit inventariseren.

Een dergelijke ervaring kan traumatische gevolgen hebben en zelfs resulteren in arbeidsongeschiktheid. Daarom enkele raadgevingen die men als slachtoffer van dergelijke feiten het best in acht neemt:

- neem ruim de tijd om over de zaak na te praten;
- luister naar elkaars angstgevoelens en verwijt niemand wat;
- vraag de politie om slachtofferhulp (doorverwijzing naar gespecialiseerde slachtofferopvang).

CARJACKING

Situering

Een carjacking is een diefstal (of poging daartoe) van een voertuig waarbij de daders t.a.v. de bestuurder of zijn passagier(s) geweld of bedreigingen gebruiken. Het is echter ook mogelijk dat zij het geweld (of de bedreiging) op het ogenblik dat zij op heterdaad worden betrapt aanwenden om in het bezit te blijven van het gestolen voertuig of om hun straffeloosheid te verzekeren.

Carjackings maken (slechts) 3,5% van het totale aantal voertuigdiefstallen uit (politie cijfers 2009). Carjackings

komen in het hele land voor, maar worden toch vooral gepleegd in de arrondissementen Brussel-Asse, Luik, Charleroi, Antwerpen en Bergen. Ongeveer de helft van de gearjackte voertuigen wordt teruggevonden.

Mocht er zich een overval voordoen, probeer kalm te blijven. Maak geen onverwachte bewegingen.

Vooraf recente voertuigen worden gestolen. Meer dan 50% van de gearjackte voertuigen is minder dan 2 jaar oud. Wagens van bedrijfsleiders (duurdere types; dikwijls geleaste voertuigen waarbij het eigendomsgevoel minder speelt) zijn zeker gegeerde doelwitten van carjackers.

Preventieve maatregelen

Er zijn een aantal preventieve maatregelen die potentiële slachtoffers kunnen nemen om zich beter te beveiligen. Deze maatregelen kunnen algemeen van aard zijn, zoals het vergrendelen van alle deuren als iedereen in de wagen heeft plaatsgenomen, het gescheiden houden van autosleutels en huissleutels, het thuis bewaren van een kopij van alle boorddocumenten.

De maatregelen kunnen ook meer specifiek zijn, zoals:

- vermijd risico's bij het in- of uitstappen van de wagen (parkeer de wagen steeds op een goed verlichte en geen afgelegen ►►

- ▶ plaats; wees alert voor mensen die u schijnbaar iets komen vragen op het moment van in- of uitstappen,...);
- vermijd risico's op de weg (houd vensters en deuren slotvast, zeker in grote steden; wees alert als u moet stoppen; kijk regelmatig of u niet gevolgd wordt; wees vooruitziend om u niet te laten klemrijden,...);
- vermijd risico's bij een al dan niet opzettelijke aanrijding (houd er rekening mee dat een aanrijding opzettelijk kan zijn om ervoor te zorgen dat u uw voertuig verlaat; wees steeds alert en vergrendel alle deuren als u meent iets verdacht waar te nemen; communiceer in een eerste tijd via het halfopen raam...);
- vermijd risico's bij een versperring van de weg (indien andere weggebruikers de rijbaan versperren, tracht toch bepaalde manoeuvreerruimte te behouden om eventueel te kunnen wegrijden,...);

Carjackings maken (slechts) 3,5% van het totale aantal voertuigdiefstallen uit (cijfers 2009).

- daarnaast kunnen ook maatregelen worden aanbevolen, gericht op het voertuig, zoals bouwkundige, elektromechanische en elektronische maatregelen, waarbij men alle mogelijke alarmsystemen kan in acht nemen. Een belangrijke evolutie hierbij is het gebruik van 'aftertheft' (nadieststal)-systemen, waarbij voertuigen via gps kunnen worden gelokaliseerd.



Hoe te reageren in geval van een incident?

Indien u toch het slachtoffer wordt van een carjacking, doe dan geen onbezonnen dingen: blijf kalm, bied geen weerstand, zoek geen fysisch contact, verwijder u van de dader(s) als u de mogelijkheid heeft, en verwittig onmiddellijk de politiediensten.

DIEFSTAL UIT VOERTUIGEN

Situering

Een diefstal van of uit uw wagen kan voor heel wat problemen zorgen. Onvoorziene kosten, administratieve rompslomp, tijdverlies en een naar gevoel zijn maar enkele van de gevolgen die een dergelijke diefstal kan teweegbrengen. Iedereen zal het er mee eens zijn dat we dergelijke dingen beter voorkomen dan genezen, maar vaak zijn de



mensen gewoon niet op de hoogte van de eenvoudige maatregelen die ze kunnen nemen. En dan hebben we het niet alleen over dure alarminstallaties.

Ieder jaar zijn er ongeveer 70.000 feiten van diefstallen uit voertuigen, wat neerkomt op 190 feiten per dag. De meeste diefstallen worden in de grote steden gepleegd waar een grotere anonimiteit heerst en waar de voertuigen in overvloed aanwezig zijn. De **top 10** van de gestolen goederen bestaat uit: tassen en portemonnee (+20%), gps, geld, bankkaarten, autoradio, cd's, rijbewijs, gsm, boorddocumenten, laptop en kleren.

Waar wij vooral uw aandacht op willen vestigen, zijn de boorddocumenten en in het bijzonder het inschrijvingsbewijs – de echte

identiteitskaart van het voertuig. Het inschrijvingsbewijs is zeer belangrijk en is ook de rode draad in de voertuigzwendel. Dankzij dit document kan een gestolen voertuig opnieuw in het legale circuit (via een inschrijving in het buitenland) gebracht worden.

Preventieve maatregelen¹⁴

- Parkeer uw wagen bij voorkeur in een garage of op een andere veilige plaats. Kies in ieder geval voor een niet afgelegen en goed verlichte parkeerplaats.
- **Sluit uw wagen steeds zorgvuldig af:** vergeet naast de portieren ook niet de ramen, het open dak en het kofferdeksel goed te sluiten. Dit is belangrijk, want als u uw wagen openlaat en er wordt iets gestolen zonder braak, dan is dat in de ogen van de verzekering geen diefstal. Dit kan u tevens een fikse geldboete opleveren.
- Als u de wagen verlaat, **neem dan steeds uw boorddocumenten mee**, want deze zijn geld waard voor criminelen. Neem in geval van een langere afwezigheid systematisch deze voorzorg¹⁵.
- **Verwijder steeds uw mobiele gps en gps-houder uit de wagen. Veeg ook de zuignapafdruk weg** op uw voorruit. Dieven breken in uw wagen in bij het zien van een gps en/of gps-houder en/of zuignapafdruk op uw raam, in de hoop zich een gps toe te eigenen.
- **Schakel steeds de bluetooth en wifi-functie uit** (van uw gps, laptop, gsm...) ►►

¹⁴ De brochure 'Voorkom diefstal uit je auto', FOD Binnenlandse Zaken, kunt u raadplegen op www.besafe.be.

¹⁵ Op www.besafe.be kunt u gratis een boorddocumenthouder bestellen, alsook de preventiebrochures.



- ▶▶ opdat potentiële dieven dit signaal niet zouden kunnen opvangen en zo weet krijgen van aanwezigheid van uw waardevolle voorwerpen.
- Indien niets waardevols aanwezig is in het voertuig, toon dit: laat uw handschoenkastje en/of kofferzeil open.

Als u de wagen verlaat, neem dan steeds uw boorddocumenten mee, want deze zijn geld waard voor criminelen.

- Voorwerpen die (per uitzondering) toch in de auto blijven liggen, kunnen bij voorkeur in de afgesloten koffer opgeborgen worden. **Leg het voorwerp bij vertrek in uw koffer** en niet op de plaats van bestemming, zodat een potentiële dief deze handeling niet ziet.
- Hou een inventaris bij van de serienummers, merk en type van al uw waardevolle voorwerpen (voorbeeld op www.besafe.be). Doe dit ook voor uw gps, laptop, imei-nr. van je gsm,... Het serienummer en imei-nr. zijn unieke nummers waardoor de politie de teruggevonden gestolen goederen vlugger kan toewijzen

en terugbezorgen aan de rechtmatige eigenaar.

- **Gebruik de pincode op uw gps.**

Deze optie is vaak voorzien, maar niet standaard geïnstalleerd. Stel deze functie in, na diefstal kan uw gps niet meer gebruikt worden zonder de juiste pincode.

Specifiek voor het inschrijvingsbewijs

Voor de leasing/huurvoertuigen zijn er twee inschrijvingsbewijzen in omloop per voertuig:

1. het origineel (wordt gewoonlijk bewaard op de hoofdzetel van het bedrijf) of duplicaat (in geval van verlies of diefstal van het origineel);
2. het afschrift (volgt meestal het voertuig en is dus in het bezit van de huurder - zie illustratie p. 39); het gaat om een authentiek document waarop de volgende gegevens zijn aangebracht:
 - a. voertuig bestemd om verhuurd te worden - afschrift
 - b. opgemaakt ten gerieve van de huurder van het voertuig
 - c. afschrift niet geldig bij verkoop van het voertuig!

We raden leasing- of verhuurmaatschappijen sterk aan om gebruik te maken van het afschrift. Het kan gratis gevraagd worden bij de Dienst Inschrijvingen Voertuig (DIV) bij de inschrijving.

Hoe te reageren in geval van een incident?

Als u, ondanks alle voorzorgen, toch nog het slachtoffer wordt van diefstal, ga dan



zo vlug mogelijk naar een politiedienst, indien mogelijk met de identificatiefiche¹⁶ van uw voertuig bij de hand.

Bij diefstal van boorddocumenten is het nog meer aangewezen om aangifte te doen bij de lokale politie. Zonder aangifte ga je geen duplicaat van een inschrijvingsbewijs kunnen vragen bij de Dienst Inschrijvingen Voertuig (DIV).

Nog een rede te meer om aangifte te doen: de politiemann gaat het gestolen inschrijvingsbewijs seinen. Dit betekent dat als er iemand in het buitenland aan de hand van uw gestolen inschrijvingsbewijs een ander voertuig wil inschrijven, hij verhinderd zal worden. Op die manier kan er geen misbruik worden gemaakt van uw document.

VANDALISME

Situering

Vandalisme is een van de meest voorkomende vormen van criminaliteit. Het probleem vindt meestal zijn oorsprong buiten het bedrijf. Naar de toekomst toe ver-

wachten de meeste bedrijven dat dit cijfer vrij stabiel blijft.

Vandalisme is een typisch jongerendelict. Vaak gaat het om jongens (in mindere mate om meisjes) in de leeftijd van 8 tot 16 jaar. Ze brengen moedwillig vernielingen of beschadigingen aan, zonder dat ze daar in materieel opzicht iets mee opschieten. Het gaat ze puur om het vernielen of beschadigen zelf. Hierdoor verkennen ze hun grenzen en proberen ze de wereld van de volwassenen te tarten. Vandalisme stelt ze vaak in hoger aanzien bij hun vriendengroep.

Veel maatregelen tegen vandalisme worden getroffen door onderwijsinstellingen en door organisaties voor jeugdwerk. Ook door het opleggen van alternatieve straffen worden veel problemen in de kiem gesmoord.

Wanneer u als ondernemer maatregelen wilt treffen, is het belangrijk om twee kenmerken goed in het oog te houden. Vandalisme is een impulsdelict: de gelegenheid maakt de vandaal. Bovendien is vandalisme een sociaal delict. Het wordt bijna ►►

¹⁶ Voorbeeld op www.besafe.be.

- ▶▶ altijd in groepsverband gepleegd. Niettegenstaande dat het potentiële slachtofferchap van vandalisme hoog scoort, nemen bedrijven nauwelijks specifieke maatregelen om zich tegen deze vorm van criminaliteit te beschermen. Interne bewaking (en in mindere mate externe bewaking) draagt

Veel problemen met vandalisme kunnen voorkomen worden door de informele controle in de directe omgeving van uw bedrijf te versterken.

onrechtstreeks bij tot een verlaging van het risico. Het zijn vaak grotere bedrijven, die reeds geconfronteerd werden met feiten van sabotage, vandalisme of diefstal, die overgaan tot dergelijke beveiligingsmaatregelen.

Preventieve maatregelen

U kunt veel problemen met vandalisme voorkomen door de **informele controle** in de directe omgeving van uw bedrijf te versterken. Daarbij kunt u denken aan verschillende mogelijkheden:

- het houden van schoonmaakacties in samenwerking met de reinigingsdienst in uw gemeente en in samenwerking met de bewoners (jong en oud) in uw buurt;
- bijdragen aan de organisatie van feestelijke activiteiten in uw buurt om daarmee de betrokkenheid van de bewoners bij uw omgeving te versterken;
- jongeren betrekken bij de inrichting van uw omgeving, bijvoorbeeld bij schilderwerk van rolluiken of schuttingen die anders voortdurend beklad worden.

U kunt ook de **formele controle** versterken, bijvoorbeeld met behulp van een bewakingsfirma.



Ook met behulp van **aanpassingen van de fysieke omgeving** van uw bedrijf kunt u problemen voorkomen. U kunt daarbij de volgende maatregelen treffen:

- zorg voor een goed onderhoud en herstel snel de aangerichte vernielingen;
- verstevig kwetsbare objecten, bijvoorbeeld door slagvast glas en kunststof te gebruiken. Bedenk echter dat verstevigde objecten ook een extra uitdaging kunnen inhouden om ze toch kapot te krijgen. Bovendien zijn verstevigde objecten vaak duurder; waardoor de schade van vandalisme groter wordt;
- bescherm kwetsbare objecten, bijvoorbeeld met behulp van beplanting, met rolluiken of met traliewerk;
- verfraai kwetsbare objecten, bijvoorbeeld door afwisselend kleurgebruik of door een reliëfstructuur aan te brengen op gladde muren en deuren;
- verwijder kwetsbare objecten.

Ten slotte kunt u met de **ruimtelijke inrichting van de omgeving** rond uw bedrijf het probleem van vandalisme tegengaan. Zo is het aan te raden om te zorgen voor een goed zicht op de ruimte rond uw bedrijf. Daarmee voorkomt u dat er typische 'rondhangplekken' ontstaan waar groepen jongeren zich verzamelen.

Hoe te reageren in geval van een incident?

Uiteraard is het ook hier aangewezen **steeds** aangifte te doen bij de lokale politie, die uw gesprekspartner bij uitstek is in geval van dergelijke incidenten.

Vandalisme, beschadigingen en graffiti kunnen ook online aangegeven worden via het virtuele loket van de politie via **www.Police-on-web.be**. Meer uitleg hieromtrent vindt u in het punt 4 van deze brochure. ●



2

Early warning system: een bedrijfsinformatienetwerk tegen terroristische dreigingen

WAT IS HET 'EARLY WARNING SYSTEM'?

Sinds 6 maart 2009 startte formeel een bedrijfsinformatienetwerk tegen terroristische dreigingen in ons land. Bedrijven en overheidsdiensten zullen via een vaste procedure informatie uitwisselen om de economische sector en zijn personeelsleden zo goed mogelijk te beschermen tegen eventuele terroristische aanslagen.

De Federale Overheidsdiensten van Justitie en Binnenlandse Zaken hebben het informa-

tiernetwerk opgezet in nauwe samenwerking met het Verbond van Belgische Ondernemingen. Het protocol daarover werd op 6 maart 2009 ondertekend door de minister van Justitie Stefaan De Clerck, de minister van Binnenlandse Zaken Guido De Padt, en de gedelegeerd bestuurder van het Verbond van Belgische Ondernemingen Rudi Thomaes.

Het informatienetwerk is een deeltje van het veel uitgebreider arsenaal dat de overheid al eerder in werking heeft gesteld in de strijd tegen het terrorisme (van gerechtelijke onderzoeken tot het Orgaan voor de

Coördinatie en de Analyse van de Dreiging of OCAD).

Bedoeling is dat een bedrijf dat bijvoorbeeld aan zijn toegangspoort dagen na elkaar dezelfde wagen ziet halt houden, de overheid daarover inlicht zodat dit kan worden onderzocht. Blijkt het incident echt verdacht, of heeft een ander bedrijf bijvoorbeeld dezelfde feiten met dezelfde wagen vastgesteld, dan kan via het netwerk een hele sector worden gewaarschuwd. Omgekeerd zal de overheid, als er bijvoorbeeld een algemene dreiging is uitgesproken tegen een bepaalde bedrijfssector, die sector waarschuwen.

De uitwisseling van informatie over verdachte elementen gebeurt in een vroeg stadium – ‘early warning’ –, zodat de aard van de dreiging snel kan worden onderzocht. Door het samenbrengen van informatie kunnen verdachte handelingen of dreigingen ook in een juiste context worden geplaatst. Wellicht zal blijken dat het overgrote deel van deze verdachte handelingen niets te maken heeft met een extreme dreiging.

VOOR EN DOOR WIE?

De informatiestroom loopt tussen vaste partners van de publieke en de private sector.

Langs de kant van de Belgische bedrijven speelt het VBO een cruciale rol om de informatie gericht te verspreiden.

Langs overheidszijde zijn de belangrijkste partners:

- de Algemene Directie van het Crisiscentrum (FOD Binnenlandse Zaken);
- de Veiligheid van de Staat (FOD Justitie);
- de Federale politie;
- het Coördinatieorgaan voor de Dreigingsanalyse (OCAD);
- het Federaal parket.

Het netwerk wordt op initiatief van zowel de publieke als de private partners gevoerd: er wordt (geanonimiseerde) informatie uitgewisseld over verdachte handelingen of incidenten vastgesteld bij de ondernemingen of over mogelijke bedreigingen die door de overheid worden onderzocht.

WAT NIET?

Het informatienetwerk wordt niet gebruikt om systematisch alle mogelijke dreigingen en incidenten voor de openbare orde en veiligheid te communiceren.

Evenmin is het de bedoeling van dit netwerk om in de plaats te treden van de normale communicatie tussen plaatselijke bedrijven en de lokale politie.

HOE?

Via een permanent centraal contactpunt onderhouden de nationale verantwoordelijken van bedrijven contacten met de diensten die op nationaal vlak belast zijn met de strijd tegen het terrorisme. ►►

VBO ALERT CONTACT POINT

E-mail: VBOalert@belgacom.be

Telefoon: 0800/91.777

Indien dit nummer om uiteenlopende redenen onbereikbaar is, kan gebruik worden gemaakt van de volgende mogelijkheden:

Noodlijn: 02 202 18 00

Niet-PABX lijnen: 02 202 61 24 en 02 202 61 25

Fax: 02 202 63 29

- Het systeem heeft al een geslaagde testperiode achter de rug en zal ook in de toekomst regelmatig geëvalueerd worden om het systeem efficiënt te houden.

PUBLIEK-PRIVATE SAMENWERKING

Het protocolakkoord tussen de publieke en private partners werd operationeel op 6 maart 2009, na de ondertekening door de ministers van Justitie en Bin-

De publiek-private samenwerking is een initiatief van het Permanent Overlegplatform Bedrijfsbeveiliging.

nenlandse Zaken en de gedelegeerd bestuurder van het Verbond van Belgische Ondernemingen.

Deze vorm van publiek-private samenwerking is een initiatief van het Permanent

Overlegplatform Bedrijfsbeveiliging dat door de Dienst voor het Strafrechtelijk beleid van de FOD Justitie sinds vele jaren wordt voorgezeten.

Bijkomende informatie kan verkregen worden via de commissie Bedrijfsbeveiliging van het VBO, hetzij bij Christine Darville, coördinator van deze VBO-commissie, of bij Gilbert Geudens, voorzitter van deze commissie.

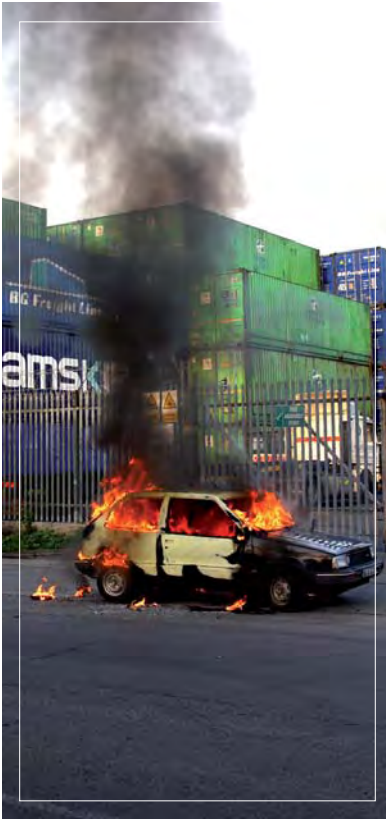
WERKING VAN HET INFORMATIEVIERKANT

Het informatievierkant heeft tot doel om relevante informatie in het kader van een (mogelijke) terroristische dreiging uit te wisselen tussen de private en publieke sector.

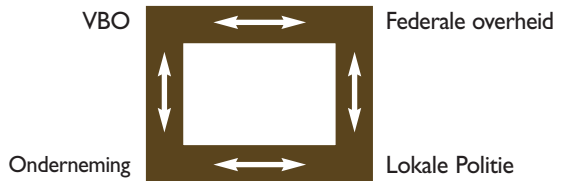
Het informatievierkant is aanvullend aan de bestaande politiekanaalen: meldingen van verdachte situaties of dreigingen ten aanzien van een onderneming dienen dus steeds via de lokale politie te gebeuren. Die zal op zijn beurt de informatie over-

maken aan de federale autoriteiten, waar o.a. een grondige analyse van de informatie wordt gemaakt.

Bijkomend kan de onderneming deze informatie nu ook overmaken aan een nationaal contactpunt, georganiseerd door het bedrijfsleven. Dit contactpunt zal eveneens de informatie doorgeven aan de federale autoriteiten. Op die manier is er dus een 'early warning system' opgestart voor potentieel relevante informatie vanuit het bedrijfsleven.



Omgekeerd kan de overheid (naast de infodoorstroming naar en via de lokale politie) via het nationaal contactpunt één of meerdere sectoren informeren over een specifieke situatie of dreiging met het oog op een verhoogde waakzaamheid of bijkomende veiligheidsmaatregelen.

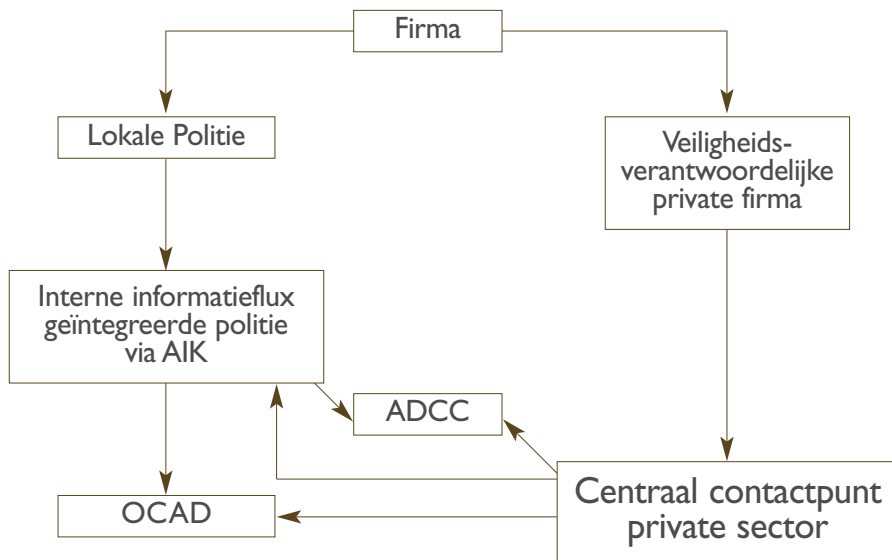


VOORBEELDEN VAN TOEPASSINGEN VAN HET INFORMATIEVIERTAKT EN/OF HET CONTACTPUNT

- Verdachte bewegingen omheen een bedrijf(sterrein).
- Anonieme meldingen gericht aan een onderneming.
- Een gevoelige samenshoring aan de bedrijfspoorten.
- Feedback aan het bedrijfsleven omtrent (vermeende) verdachte handelingen.
- Verschaffen van specifieke bedrijfs- of sectorgegevens (bv. contactgegevens van veiligheidsverantwoordelijken) aan de overheid. ►►

VOORBEELD I:

►► BOMALARM - INCIDENT – VERDACHTE HANDELING / PRIVATE SECTOR VERSUS PUBLIEKE SECTOR



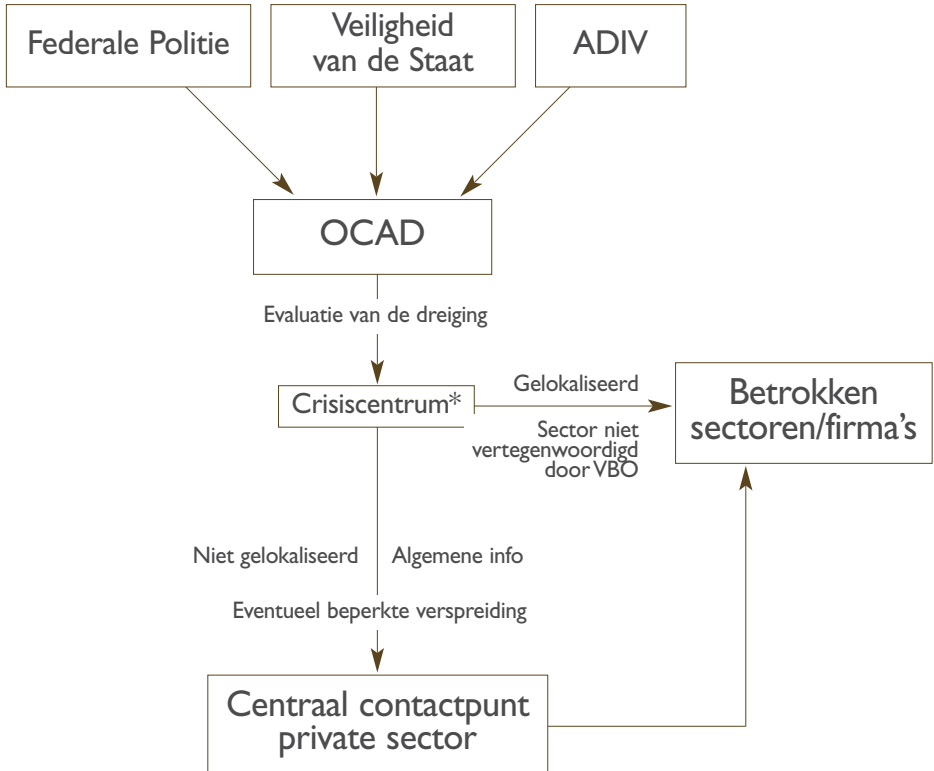
Legende:

AIK: Arrondissementeel Informatie Kruispunt van de Federale Politie

ADCC: Algemene Directie CrisisCentrum

OCAD: Orgaan voor de Coördinatie en de Analyse van de Dreiging

VOORBEELD 2:

**BEDREIGINGEN – AANBEVELINGEN PUBLIEKE SECTOR
VERSUS PRIVATE SECTOR**


(*ook informatiedoorstroming naar Federale Politie via geëigende kanalen)

Wanneer de private sector van het moederbedrijf in het buitenland verneemt dat de beveiligingsmaatregelen moeten worden opgevoerd, kan via het centrale meldpunt een cross-check van de private naar de publieke sector plaatsvinden. ●

Legende:

ADIV: Algemene Dienst Inlichtingen en Veiligheid van het leger

OCAD: Orgaan voor de Coördinatie en de Analyse van de Dreiging



3 Technopreventieve adviezen¹⁷

WAT IS TECHNOPREVENTIE?

Technopreventie heeft als doel inbraak, gawdiefstal en overvallen te voorkomen. Deze discipline bevat drie soorten beveiligingsmaatregelen die altijd in deze volgorde worden behandeld:

- a. de organisatorische maatregelen;
- b. de mechanische (bouwkundige) maatregelen;
- c. de elektronische maatregelen.

Deze maatregelen kunnen de kans om slachtoffer te worden van een inbraak, diefstal of overval aanzienlijk verminderen.

a. Organisatorische maatregelen

Veiligheid begint met het aannemen van goede gewoonten. Deze maatregelen kunnen door iedereen worden toegepast, ze zijn goedkoop en zo eenvoudig dat ze vaak over het hoofd worden gezien. Niettemin vormen ze de eerste en essentiële stap van ons beveiligingsplan. Voorbeelden: goed sleutelbeheer; registreren van waardevolle voorwerpen, deuren en ramen met sleutel sluiten, zelfs bij korte afwezigheid,...

b. Bouwkundige maatregelen

U kan de ramen en deuren van uw handelszaak verstevigen teneinde het de inbreker zeer moeilijk te maken¹⁸.

Voorbeelden: veiligheidsglas, inbraakwerende rolluiken, beveiligingsystemen voor deuren, ramen, luiken, garagepoorten, lichtkoepels, dakvensters, keldergaten en hekken zoals veiligheidssloten, slotbeveiligingsystemen, grendelbeveiligingsystemen en kierstandhouders, kluis,...

c. Elektronische maatregelen

Het plaatsen van een elektronisch veiligheidssysteem moet in combinatie gebeuren met voorafgaande organisatorische en technische maatregelen. Elektronische maatregelen zijn dus een aanvulling op de organisatorische en technische maatregelen. Voorbeelden: alarmsysteem, camerasysteem¹⁹, volgsysteem. Op p. 50 krijgt u meer uitleg over de camerabewaking.

Weet u trouwens dat de overheid de zelfstandige en de vrije beroepen steunt wanneer ze veiligheidsinvesteringen nemen in hun zaak, door een verhoogde fiscale aftrek toe te kennen? Meer informatie hierover vindt u bij de technopreventief adviseur van uw politiezone²⁰.

WAT IS EEN TECHNO-PREVENTIEF ADVISEUR?

Een technopreventief adviseur werkt bij de gemeente of politie, is erkend door

de Federale Overheidsdienst Binnenlandse Zaken en opgeleid om gratis en neutraal advies te geven inzake technopreventie.

WAT IS DE ROL VAN DE TECHNOPREVENTIEF ADVISEUR?

De voornaamste opdrachten van de technopreventief adviseur (TPA) zijn:

- a. objectief en volledig kosteloos advies geven over inbraakbeveiliging;
- b. preventieadvies geven aan de kandidaat-bouwers of mensen die een woning renoveren, soms op basis van door de architect gemaakte plannen (op uw vraag);
- c. adviseren van zelfstandigen, handelaars, uitoefenaars van vrije beroepen,... over de beveiliging tegen inbraak/overvallen/winkeldiefstal;
- d. geven van uitleg/conferenties over criminaliteitspreventie aan verschillende doelgroepen (op vraag van burgergroeperingen, wijkverenigingen, handelaarsverenigingen, beroepsverenigingen,...);
- e. aanreiken van relevante en actuele informatie over technopreventief materiaal en over verschillende beveiligings- en preventietechnieken.



¹⁷ Bron: www.besafe.be.

¹⁸ Alle info op www.veiligewoning.be.

¹⁹ Wet van 21 maart 2007- www.privacycommission.be.

²⁰ Of op www.besafe.be - rubriek 'Ondernemers'.

► HOE KOM IK IN CONTACT MET DE DICHTSTBIJZIJNDE TECHNO-PREVENTIEF ADVISEUR?

Op www.besafe.be kan via een zoekmotor per postcode gezocht worden naar een technopreventief adviseur. Aarzel niet om contact met hem/haar op te nemen en een afspraak te maken. Denk eraan dat het om een professionele, objectieve en volledig KOSTELOZE dienstverlening gaat.

CAMERABEWAKING

Naast de wettelijke voorwaarden is het eveneens van belang dat de beelden kunnen aangewend worden om de daders van de diefstal op te sporen.



Het gebruik van camerabewaking wordt geregeld door de wet van 21 maart 2007, waarbij een onderscheid wordt gemaakt tussen drie categorieën van plaatsen, nl. niet-besloten plaatsen (bv. plein), besloten plaatsen toegankelijk voor het publiek (bv.

winkel) en besloten plaatsen niet toegankelijk voor het publiek (bv. bedrijf, opslagruimte).

Voor de ingebruikname van de camerabewaking dient aan een aantal formaliteiten voldaan te worden. Hieronder vindt u de **checklist voor camerabewaking op publiek toegankelijke besloten plaatsen, door middel van VASTE bewakingscamera's**.

Checklist voor camerabewaking op publiek toegankelijke besloten plaatsen.

- Is er duidelijk bepaald voor welke doelstelling(en) camerabewaking wordt ingezet? Beantwoordt de plaatsing en het gebruik aan de in de wet van 8 december 1992 (privacywet) bepaalde beginselen? Met andere woorden:
 - **beginsel van finaliteit:** is er formeel bepaald welke veiligheidsdoelstellingen bereikt willen worden? Opgelet: u kan enkel de beelden gebruiken in het kader van de opgegeven finaliteit;
 - **beginsel van subsidiariteit:** kan u motiveren dat een camerasysteem het gepaste en het noodzakelijke middel is om uw veiligheidsdoelstellingen te bereiken?
 - **beginsel van proportionaliteit:** kan u motiveren dat er een evenwicht is tussen de verhoging van de veiligheid en de impact op het recht op bescherming van de persoonlijke levenssfeer?
- Is er aangifte gedaan aan de Privacycommissie²¹, uiterlijk de dag vóór de dag dat de bewakingscamera's in gebruik worden genomen?

- Is er aangifte gedaan aan de korpschef van de betreffende politiezone, uiterlijk de dag vóór de dag dat de bewakingscamera's in gebruik worden genomen?
- Is er een pictogram geplaatst aan de toegang tot de publiek toegankelijk besloten plaats dat aangeeft dat er camerabewaking plaatsvindt?
- Zijn de camera's uitsluitend gericht op plaatsen waarvoor de beheerder zelf de gegevens verwerkt?
- Gebeurt het 'real time' bekijken van de beelden uitsluitend om onmiddellijk te kunnen ingrijpen bij misdrijven, schade of ordeverstoring?
- Is het opnemen van beelden uitsluitend gericht op het verzamelen van bewijzen van overlast of van feiten die een misdrijf opleveren of schade veroorzaken en om daders, ordeverstoorders, een getuige of een slachtoffer op te sporen of te identificeren?
- Worden de beelden niet langer dan één maand bewaard indien zij geen bijdrage leveren tot het bewijzen van een misdrijf, van schade of van overlast of tot het identificeren van een dader, een ordeverstoorder, een getuige of een slachtoffer?
- Zijn de nodige voorzorgsmaatregelen genomen teneinde de toegang tot de beelden te beveiligen tegen toegang voor onbevoegden?
- Leveren de bewakingscamera's geen beelden op die de intimiteit van een persoon schenden, zijn ze niet gericht op het inwinnen van informatie over de filosofische,

religieuze, politieke, syndicale gezindheid, etnische of sociale origine, het seksuele leven of de gezondheidstoestand?

Een pictogram moet aangeven dat er camerabewaking plaatsvindt.

Alsnog enkele tips voor een goede plaatsing van de camera(s):

- hang de camera op ooghoogte en zorg ervoor dat belemmerende voorwerpen worden vermeden (bv. reclamezuilen);
- tegenlicht en spiegelingen spelen eveneens in op de kwaliteit van de beelden;
- doe een dagelijkse test zodat de plaatsing u correct voorkomt en check bij sluitings-tijd of de camera niet beschadigd, verdraaid of afgedekt is;
- zorg dat het personeel weet waar de camera hangt en hoe de camera moet worden gebruikt;
- zet de registratieapparatuur op een veilige plaats (onzichtbaar en in afgesloten kast/ruimte);
- controleer regelmatig de kwaliteit van de opnames.

ANDERE BEVEILIGINGSMAAAT-REGELLEN

Voor andere beveiligingsmaatregelen zoals volgsystemen, alarmsystemen, enz. verwijzen we u graag door naar de site van de FOD Binnenlandse Zaken²².

²¹ www.privacycommission.be/elg/cameraMain.htm - 'thematische aangifte'.

²² www.vigilis.be.



4 Nuttige links en websites

POLICE ON WEB



www.Police-on-web.be is het virtuele loket van de politie of een elektronisch loket waar u, enerzijds, online klacht indient voor misdrijven uit onderstaande lijst en een bericht van afwezigheid instelt, en, anderzijds, uw alarmsysteem meldt.

Police on web laat de burger en de bedrijven toe om bepaalde klachten te registreren zonder via het politiekantoor langs te gaan. De klachten kunnen dus 7d/7 en 24u/24 neergelegd worden via eender welke pc met een internetverbinding en dit voor volgende feiten:

- fietsdiefstal;
- bromfietsdiefstal;
- winkeldiefstal;
- diverse beschadigingen;
- graffiti.

Om een klacht in te dienen, moet je je identificeren aan de hand van:

- een elektronische identiteitskaart en eID kaartlezer en een computer met internetverbinding;
- een 'Token': is een kaartje (afmeting van een bankkaart) dat 24 persoonlijke codes bevat die via de federale portaal-site.be te verkrijgen is;
- een account op de federale portaal-site.be die kan gecreëerd worden aan de hand van uw Rijksregisternummer, uw SIS-kaartnummer en uw identiteitskaartnummer.

eCOPS


Belgisch overheidsmeldpunt voor internetmisbruik

eCops is een online meldpunt waar u als internetgebruiker misdrijven op of via het internet kan melden. U hoeft zich niet te bekommeren over 'Wie is er nu juist bevoegd?'. eCops zorgt ervoor dat uw melding door de bevoegde dienst wordt onderzocht.

Kwam u terecht op een verwarrende site met misleidende informatie? Ontving u via e-mail ongewenste reclame of een frauduleus voorstel? Zag u kinderporno op een site?

Uw melding kan de aanleiding zijn voor een verdere actie door de FOD Economie, Politie of Justitie. U doet uw melding stap voor stap via het online meldingsformulier op www.ecops.be.

eCops is geen online centrale voor noodoproepen aan de Politie!

CHECKDOC


Internetsite voor het verifiëren van Belgische identiteitsdocumenten (paspoort, identiteitskaart, verblijfstitel met chip)

De site www.checkdoc.be is een internet-

site die iedereen in staat stelt om – kosteloos en in real time – overal ter wereld te verifiëren of een Belgisch identiteitsdocument dat hem wordt voorgelegd, wel degelijk is uitgereikt en niet bekendstaat als verloren, gestolen, verlopen of ongeldig. De gebruiker kan een autoverhuurder zijn, of een bank, een hotel, een notaris, een handelaar:

www.checkdoc.be is een zoekmotor die een opzoeking uitvoert bij het Rijksregister en de databank van de paspoorten, op basis van het identificatienummer van het voorgelegde document. Binnen enkele seconden ontvangt de gebruiker een antwoord in de vorm van een 'HIT' of 'NO HIT'. Hierdoor kan de gebruiker een veiligere beslissing nemen.

Checkdoc.be gebruiken is heel eenvoudig! De eerste keer moet u zich registreren door een inschrijvingsformulier in te vullen en door de gebruiksvoorwaarden van de site te aanvaarden. U ontvangt dan een activeringscode op het e-mailadres dat in het formulier vermeld staat (en dat uw gebruikersnaam is).

Om een verificatie uit te voeren in www.checkdoc.be, moet u zich identificeren (login) en dan heeft u de keuze tussen twee formules: een didactisch 'basic' formule, en een snelle 'expert' formule.

- In de 'basic' formule wordt u geholpen bij het selecteren van het document aan de hand van foto's die de plaats van het nummer tonen dat moet worden ingegeven. ►►

- ▶ In de 'expert' formule krijgt u al een antwoord in 2 muisklikken.

HIT / NO HIT

- **HIT:** als het document dat u verifieert bij de Belgische overheden bekendstaat als gestolen, verloren, verlopen of ongeldig of als een document met dit nummer niet door deze overheden werd uitgereikt. De reden van deze 'hit' wordt niet aan u meegedeeld.
- **NO HIT:** boodschap die door de site CHECKDOC aan de gebruiker wordt gestuurd als het document dat u verifieert wel degelijk door een Belgische overheid werd uitgereikt en niet bekendstaat als gestolen, verloren, verlopen of ongeldig.

Wees waakzaam en spoor valse documenten op! Checkdoc.be geeft u ook praktische tips voor het verifiëren van de veiligheidselementen van de Belgische identiteitsdocumenten.

DOCSTOP



DOCSTOP is een helpdesk die het voor iedere houder van een Belgisch identiteitsdocument mogelijk maakt om, waar ook ter wereld, 24 uur op 24, het verlies of de diefstal van zijn identiteits- of reisdocumenten te melden. Hiervoor kan hij overal ter wereld gebruik maken van



het gratis nummer 00800 2123 2123 (in landen waar het 00800-nummer niet bereikbaar is, moet u bellen naar + 32 2 518 2123).

Eerst gaat men de identiteit van de beller na om te zien of het wel degelijk de titularis van het document is. Daarna blokkeert de operator onmiddellijk de documenten. Vanaf dat ogenblik zal iedere verificatie op **www.checkdoc.be** aanleiding geven tot een 'HIT' zonder te moeten wachten tot de titularis een aanvraag voor een nieuw identiteitsdocument doet. De burger vermijdt zo dat hij het slachtoffer wordt van een frauduleus gebruik van zijn identiteitsdocumenten (zoals het huren van een auto, een aankoop per post, een lening op zijn naam).

DOCSTOP is een gratis dienst, 24u/24u en 7 dagen per week bereikbaar. Belangrijk: met DOCSTOP kunnen enkel Belgische identiteitsdocumenten worden geblokkeerd.



Diefstal of verlies: wat te doen?

- In geval van diefstal: bel onmiddellijk naar DOCSTOP. Doe ook aangifte van de diefstal bij het dichtstbijzijnde politiebureau of bij uw lokale politie.
- In geval van verlies: bel onmiddellijk naar DOCSTOP. Ga vervolgens naar uw gemeentehuis. Buiten de openingstijden kunt u bij de politie terecht voor een voorlopig attest.

Belangrijk: als het verloren document een verblijfstitel betreft, dient u altijd eerst aangifte van het verlies te doen bij de politie alvorens naar het gemeentehuis te gaan.

Wat gebeurt er na uw telefoontje?

- Identiteitskaarten en verblijfstitels: u ontvangt een brief waarin uw melding van verlies of diefstal wordt bevestigd. Indien u uw document terugvindt, heeft u 7 dagen de tijd, gerekend vanaf uw telefoontje, om dit te deblokken. Na die termijn wordt het identiteitsdocu-

ment ongeldig verklaard en moet u een nieuw document aanvragen bij uw gemeentehuis.

Als het verloren document een verblijfstitel betreft, dient u altijd eerst aangifte van het verlies te doen bij de politie alvorens naar het gemeentehuis te gaan.

- Paspoorten: vanaf het moment dat u DOCSTOP belt, wordt uw paspoort ongeldig verklaard. Indien u dit nodig heeft om te reizen, vraag dan op tijd een nieuw aan bij uw gemeentehuis. ●

CHECKLIST

Telefonische oproep bommelding/afpersing

Datum en uur oproep		Uur einde oproep				
Inhoud van de melding						
Is er een plaatsaanduiding?		Indien Ja, waar				
Is er een tijdsaanduiding?		Indien Ja, uur				
Uitzicht	Pakje <input type="checkbox"/>	Voertuig <input type="checkbox"/>	Niet vermeld <input type="checkbox"/>	Andere		
Soort	Bom <input type="checkbox"/>	Springtuig <input type="checkbox"/>	Niet vermeld <input type="checkbox"/>	Andere		
Reden						
Identiteit	Man <input type="checkbox"/>	Vrouw <input type="checkbox"/>	Kind <input type="checkbox"/>	Volwassene <input type="checkbox"/>	Mogelijke leeftijd	
Stem	Zacht <input type="checkbox"/>	Zwaar <input type="checkbox"/>	Hoog <input type="checkbox"/>	Diep <input type="checkbox"/>	Bitsig <input type="checkbox"/>	Dronken <input type="checkbox"/>
	Accent	Plaatselijk <input type="checkbox"/>	Gewestelijk <input type="checkbox"/>	Vreemd <input type="checkbox"/>	Andere <input type="checkbox"/>	

Uitspraak	Snel <input type="checkbox"/>	Traag <input type="checkbox"/>	Duidelijk <input type="checkbox"/>	Vervormd <input type="checkbox"/>
	Stamelend <input type="checkbox"/>	Neusklink <input type="checkbox"/>	Brabbelen <input type="checkbox"/>	Lispelend <input type="checkbox"/>
Taal	Goed <input type="checkbox"/>	Middelmatig <input type="checkbox"/>	Gemeen <input type="checkbox"/>	

Wijze	Kalm <input type="checkbox"/>	Opgewonden <input type="checkbox"/>	Gejaagd <input type="checkbox"/>	Vrolijk <input type="checkbox"/>	Dronken <input type="checkbox"/>
--------------	-------------------------------	-------------------------------------	----------------------------------	----------------------------------	----------------------------------

Achtergrondgeluiden	Machines <input type="checkbox"/>	Auto's <input type="checkbox"/>	Treinen <input type="checkbox"/>	Dieren <input type="checkbox"/>
	Straatrumoer <input type="checkbox"/>	Feeststemming <input type="checkbox"/>	Vliegtuig <input type="checkbox"/>	Muziek <input type="checkbox"/>

Aanvullende info	
-------------------------	--

Ontvanger van het bericht	
----------------------------------	--

Is het gesprek opgenomen?	
----------------------------------	--

Tips en ideeën
voor bedrijfsbeveiliging

BETER VOORKOMEN DAN GENEZEN!

Criminaliteit is een fenomeen waar Belgische ondernemingen niet aan ontsnappen. Het verwaarlozen van criminele risico's kan belangrijke schade toebrengen aan een bedrijf. Het is in deze context dat het Verbond van Belgische Ondernemingen (VBO) in samenwerking met de Federale Gerechtelijke Politie deze brochure heeft opgesteld om u te sensibiliseren naar preventie toe. Naast een algemene sensibilisatie omtrent specifieke beveiligingsproblemen wil deze brochure een aantal praktische tips en adviezen aanreiken die kunnen bijdragen tot het opstarten of verbeteren van uw beveiligingsprocedures met het oog op een verhoogde beveiliging van en in uw bedrijf.



VBO vzw

Ravensteinstraat 4
1000 Brussel
T + 32 2 515 08 11
F + 32 2 515 09 99
info@vbo-feb.be
www.vbo.be