

# WELKE MAATREGELEN KAN MIJN BEDRIJF NEMEN?

**U wilt meer weten over het antwoord op bovenstaande vraag. Hieronder volgt eerst de tekst van de website, daarna vindt u uitgebreidere informatie. Deze informatie is gebaseerd op de 'Handreiking voor bedrijven. Wat kan uw bedrijf ondernemen tegen terrorisme?', hoofdstuk 5. De handreiking kunt u downloaden of bestellen op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven).**

U kunt veel doen om uw bedrijf tegen terroristische acties te beveiligen en om goed te reageren als een incident heeft plaatsgevonden. Veel maatregelen kan uw bedrijf al hebben genomen om criminaliteit te voorkomen. Hier besteden we vooral aandacht aan preventieve maatregelen. Deze zorgen ervoor dat een bedrijf een minder aantrekkelijk doelwit is voor terroristen. Preventieve maatregelen kunnen ook de criminaliteit beperken.

## **Voorbeelden van preventieve maatregelen voor uw gebouw zijn:**

- er is een goed toegangsbeleid ingesteld;
- er zijn veiligheidssystemen in gebruik;
- er is sterk hang- en sluitwerk aangebracht op hekken, deuren en ramen.

## **Voorbeelden van preventieve maatregelen met betrekking tot uw personeel zijn:**

- het personeel is bewust gemaakt van de risico's van criminele handelingen;
- referenties worden gecontroleerd bij het aannemen van nieuwe medewerkers;
- er worden afspraken gemaakt met extern personeel.

## **Voorbeelden van preventieve maatregelen voor omgang met informatie zijn:**

- ICT-systemen worden beveiligd;
- gevoelige informatie wordt vernietigd.

## **BEDRIJFSMAATREGELEN**

### **1. WELKE MAATREGELEN KUNT U NEMEN?**

U kunt veel doen om uw bedrijf tegen terroristische acties te beveiligen en om goed te reageren op een eventuele aanslag. In deze handreiking besteden we vooral aandacht aan preventieve maatregelen. Die zorgen ervoor dat een bedrijf een minder aantrekkelijk doelwit is voor criminelen en terroristen. Preventieve maatregelen kunnen niet alleen de kans op een terroristische aanslag verminderen, maar andere bedrijfsrisico's zoals criminaliteit beperken.

Overheden en adviesbureaus delen maatregelen verschillend in. In deze handreiking hanteren we de indeling van de veiligheidsketen. Daarbij besteden we aandacht aan maatregelen die gericht zijn op objecten en diensten, personeel en informatie.

### **Praktijk: handboek korps regiopolitie Amsterdam-Amstelland**

Het korps regiopolitie Amsterdam-Amstelland bracht in 2005 een handboek uit over de maatregelen die bedrijven kunnen nemen tegen terrorisme en criminaliteit. De brochure bevat praktische tips en adviezen die grote en kleine bedrijven kunnen helpen in de ontwikkeling, herziening of uitbreiding van hun veiligheidsbeleid. De preventieve maatregelen zijn gerangschikt op aandachtspunten voor beveiliging: gebouwen, personeel en informatie.

In 2006 selecteerde het korps regiopolitie enkele bedrijven die extra aandacht nodig hebben, zoals hotels. Het korps regiopolitie legt bedrijfsbezoeken af en brengt bedrijven in contact met de buurtregisseurs. Het korps regiopolitie treedt op als bemiddelaar en stimuleert bedrijven om zich bewust te worden van de risico's. Amsterdam-Amstelland adviseert individuele bedrijven niet over specifieke maatregelen. Hiervoor kunnen bedrijven professionele bedrijven inhuren.

Het handboek is te downloaden op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)

Elk bedrijf is uniek. De risico's waarmee bedrijven te maken krijgen, zijn dus ook uniek. Dat betekent dat elk bedrijf ook zijn eigen afweging moet maken over de maatregelen die het gaat nemen. We raden u aan u daarbij te laten adviseren. De politie kan u algemene adviezen geven. Voor advies over specifieke bedrijfsmaatregelen kunt u contact opnemen met particuliere beveiligingsadviesbureaus. Dit voorkomt een investering in dure, ineffectieve en onnodige maatregelen. De effectiviteit van maatregelen stijgt als u verschillende maatregelen tegelijk neemt. Maatregelen die zich richten op de objecten zijn effectiever als ze in samenhang worden genomen met activiteiten die zich richten op het personeel.

#### **Meer informatie over beveiligingsmaatregelen**

- Handboek Terrorisme Tegenhouden. Drempelverhogende maatregelen voor bedrijven – Korps regiopolitie Amsterdam-Amstelland. Dit handboek kunt u vinden op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)
- Protecting against terrorism – Britse veiligheidsdienst MI5. Deze brochure kunt u downloaden op [www.mi5.gov.uk](http://www.mi5.gov.uk)

Voor advies over specifieke beveiligingsmaatregelen voor uw bedrijf kunt u terecht bij particuliere beveiligingsadviseurs.

## **2. PROACTIEVE MAATREGELEN**

Proactieve maatregelen voorkomen structurele oorzaken van onveiligheid of nemen deze weg. Daarmee verdwijnt ook de dreiging of het risico. De dreiging voor een bedrijf heeft te maken met het aantrekkelijkheidsprofiel dat terroristen lijken te hanteren. Dit profiel bestaat uit verschillende bedrijfseigenschappen om te bepalen of een bedrijf aantrekkelijk kan zijn voor een terroristische activiteit. Het aantrekkelijkheidsprofiel bestaat uit elementen als de kans op veel slachtoffers, grote economische schade, grote calamiteiten, maatschappelijke onrust en aantasting van specifieke maatschappelijke waarden.

Via proactieve maatregelen kunt u proberen deze factoren te beïnvloeden voorzover dat in een open maatschappij als Nederland mogelijk is. Terroristische dreigingen kunnen we nooit helemaal uitsluiten. Daarom is het niet reëel om aan bedrijven te vragen risicovolle bedrijfsactiviteiten af te stoten. U kunt wel de risico's op een andere manier verminderen. Probeer uw bedrijf op een weinig risicovolle locatie te vestigen.

## **3. PREVENTIEVE MAATREGELEN**

Preventieve maatregelen voorkomen directe oorzaken van onveiligheid en beperken de gevolgen van eventuele inbreuken daarop. Deze maatregelen zorgen ervoor dat uw bedrijf een minder makkelijk doelwit is voor terroristen. De maatregelen richten zich op objecten en diensten (en eventueel processen), personeel en informatie. Met het beveiligen van uw objecten en diensten, zorgt u ook voor de beveiliging van uw personeel en informatie. Maar ook aanvullende personele maatregelen zijn nodig. Dure beveiligingsmaatregelen hebben weinig zin als uw werknemers ze gemakkelijk kunnen ondermijnen. Veel preventieve maatregelen kan uw bedrijf al hebben genomen om criminaliteit te voorkomen.

### **3.1 OBJECTEN EN DIENSTEN**

Kijk eens naar uw objecten en diensten door de ogen van terroristen. Zij zullen er alles aan doen om te voorkomen dat anderen hun voorbereidende handelingen opmerken. Dat beperkt immers de kans op een succesvolle aanslag. Stel uzelf dan ook de vraag of onbevoegden het gebouw makkelijk kunnen binnenkomen en of veel processen en diensten routinematig zijn. En denk bij de beveiliging van uw bedrijf aan de ruimten in het gebouw, de deuren, ramen en muren en de directe en wijdere bedrijfsomgeving van het bedrijf.

#### **Vergroting zichtbaarheid**

Veel bedrijven nemen al maatregelen om de veiligheid onder normale omstandigheden zeker te stellen. Veel van deze maatregelen hebben te maken met goed 'huisvaderschap', zoals het schoonhouden en onderhouden van de publieke en gemeenschappelijke ruimten in en rond uw bedrijf. Dit vergroot de kans dat verdachte zaken of ongebruikelijke objecten sneller opvallen.

Andere voorbeelden van maatregelen die de zichtbaarheid vergroten zijn:

- beperken van bijvoorbeeld het aantal meubelen in gemeenschappelijke ruimten;
- weghalen van obstakels of voorwerpen die het zicht op uw bedrijf belemmeren;
- regelmatig legen van vuilnisbakken of gebruik van doorzichtige vuilniszakken;
- sluiten van kasten en lege kantoren;
- schoonhouden van de omgeving van het bedrijf, zoals de parkeerplaatsen;
- vasthouden aan een vaste plaats voor bepaalde zaken. Deze maatregelen zorgen ervoor dat u weet hoe de normale situatie eruit ziet. Afwijkingen zijn dan makkelijk te constateren.

#### **Bouwtechnische maatregelen**

Bouwtechnische of bouwkundige maatregelen hebben met het object zelf te maken. Soms zijn deze activiteiten effectief om terroristen buiten uw bedrijf te houden. U vergroot er in ieder geval de weerbaarheid van uw bedrijf mee. Bovendien zijn deze maatregelen ook effectief tegen criminelen.

#### **Voorbeelden van bouwtechnische maatregelen zijn:**

- kogelwerende of slagvaste beglazing;
- goed hekwerk;
- stevig hang- en sluitwerk op hekken, deuren en ramen;
- goede verlichting.

#### **Openings- en sluitingsprocedure en toegangsbeleid**

U kan terroristen helpen als uw bedrijf of bedrijfsterrein gemakkelijk toegankelijk is. Om het hen moeilijk te maken om toegang tot uw bedrijf te krijgen, kunt u bouwtechnische maatregelen nemen. Ook kunt u aandacht besteden aan procedures voor de opening en sluiting van uw bedrijf en het toegangsbeleid.

Bij het openen en sluiten van uw bedrijf moet u erop bedacht zijn dat terroristen zich kunnen laten insluiten. Controleer dus van tevoren of er nog ramen open zijn. Tijdens de opening- en sluitingsprocedure doet u er goed aan ook de omgeving te controleren. Informeer de plaatselijke politie bij ongeregelheden.

Door een toegangsbeleid op te stellen voor medewerkers en externen (onder andere bezoekers), bepaalt u onder welke voorwaarden zij uw bedrijf mogen binnenkomen. Informeer uw personeel en bezoekers over uw toegangsbeleid. Geef bijvoorbeeld aan of er een toegangscontrole is. Laat zonder vooraanmelding niemand het bedrijf in, ook niet als de persoon bekend is, zoals een bekende leverancier. Onderdeel van de toegangscontrole kan een bagagecontrole of een onderzoek aan kleding zijn. Deze onderzoeken zijn toegestaan omdat bezoekers privaat terrein betreden. Weigeren bezoekers de controle dan is de enige sanctie dat zij uw bedrijf niet mogen betreden. Uw bedrijf kan de controle dus niet afdwingen. Bezoekers moeten toestemming verlenen tot de controle. Onder onderzoek aan de kleding hoort niet het onderzoek aan het lichaam in verband met de bescherming van de integriteit van het lichaam. Controle van bagage en aan kleding is ook bij personeel toegestaan. Deze controle moet dan opgenomen zijn in de arbeidsvoorwaarden, de arbeidsreglementen of huisregels van uw bedrijf.

Eventueel kunt u een (elektronisch) pasjessysteem invoeren. Dit zal niet voor alle bedrijven mogelijk én gewenst zijn. In dat geval is bezoekersregistratie een uitkomst: noteer de naam van de bezoeker, het bedrijf of de organisatie, het telefoonnummer en de aankomsttijd van de bezoeker. Vraag uw gasten ook altijd om zich te legitimeren met een geldig legitimatiebewijs. Een belangrijk onderdeel van het toegangsbeleid is de inzet van receptionisten en/of bewakingspersoneel. Instrueer ze goed en laat ze ongebruikelijke situaties doorgeven aan de beveiligingscoördinator.

Daarnaast kunt u de kans dat onbevoegden uw bedrijf betreden verminderen door het aantal toegangswegen te beperken of een sleutelplan in te stellen. Dat houdt in dat u het aantal sleutels beperkt en ervoor zorgt dat maar een paar mensen toegangscodes van het bedrijf kennen. Een andere mogelijkheid is uw personeel en bezoekers te autoriseren voor bepaalde bedrijfsonderdelen, zodat ze zich niet meer vrij in uw bedrijf kunnen bewegen.

### **Toegangsbeleid in een hotel of warenhuis**

In hotels of warenhuizen, waar steeds mensen in en uit lopen, is het niet handig een pasjessysteem in te stellen om de toegang te beperken. Zichtbare aanwezigheid van bijvoorbeeld bewakingspersoneel is daarom belangrijk, zowel bij de ingang als binnen het bedrijf. Mensen verdienen de voorkeur boven camera's omdat camera's makkelijk te saboteren zijn.

### **Veiligheidssystemen**

Elektronische maatregelen kunnen indringers - en dus ook terroristen - ontmoedigen of vroegtijdig opmerken. U kunt een aantal veiligheidssystemen overwegen. Een geïntegreerde inzet daarvan levert de hoogste beveiliging op.

Het is verstandig na te denken over de kosten en baten: beperkt de inzet van het veiligheidssysteem werkelijk de risico's van uw bedrijf? U kunt zich laten voorlichten door een particulier beveiligingsadviesbureau. Als u zelf aan de slag gaat is de kans aanwezig dat u investeert in een systeem dat niet de gewenste beveiliging oplevert.

Deze maatregelen zijn het overwegen waard:

- goede verlichting;
- inzet van bewakingspersoneel;
- indringerdetectiesystemen (alarmsystemen);
- (elektronische) systemen voor toegangscontrole;
- video-observatie.

De inzet van systemen heeft beperkingen. Vaak zijn systemen vooral nuttig als ze vergezeld gaan met heldere huisregels, die het personeel naleeft. Ook controle op het afgaan van een alarm is heel belangrijk. Daarnaast heeft de techniek van de systemen beperkingen. Veel camera's leveren bijvoorbeeld onvoldoende beeldkwaliteit om mensen te identificeren.

### **3.2 PERSONEEL**

Bedrijven kunnen ook slachtoffer worden van kwaadwillende personeelsleden die mogelijk bereid zijn terroristische activiteiten te ondersteunen door bijvoorbeeld informatie aan terroristen te overhandigen. U kunt hier iets tegen doen door uw medewerkers bewust te maken van het belang van beveiligingsmaatregelen. Andere preventieve personeelsmaatregelen richten zich op het aannemen van nieuwe medewerkers en op het inhuren van extern personeel.

#### **Bewustwording personeel**

Het is belangrijk dat uw personeel op de hoogte is van beveiligingsmaatregelen, omdat dit de bewustwording rond het belang van beveiliging vergroot. Bespreek de maatregelen en informeer de medewerkers als er wijzigingen zijn.

Beveiliging is een verantwoordelijkheid van alle medewerkers. Doe daar gerust een beroep op. Eventueel kunt u een bijeenkomst organiseren over de risico's die uw bedrijf loopt en op welke wijze uw bedrijf daarmee omgaat. Tijdens zulke bewustwordingstrainingen kunt u uw personeel vragen een bijdrage te leveren aan de beveiliging. Denk aan aandacht voor afgesloten bureaus, kasten en een opgeruimd bureau ('clean desk') aan het einde van elke werkdag. Vanzelfsprekend vertelt u ook wie wat moet doen in bepaalde situaties: wat zijn de procedures van uw bedrijf? U kunt deze instructies in een checklist vastleggen.

Het is erg belangrijk dat medewerkers weten bij wie ze terecht kunnen als ze ongebruikelijke handelingen of situaties signaleren. Ook moeten ze erop kunnen vertrouwen dat de beveiligingscoördinator actie onderneemt naar aanleiding van hun signalen.

Werknemers die al bij u werken kunt u tijdens functionerings- en beoordelingsgesprekken wijzen op het belang van beveiliging. Daarbij kunt u ook aangeven welke sancties volgen als zij niet volgens de voorschriften handelen. Eventueel kunt u een gedragscode opstellen.

Het is mogelijk dat personeel dat al bij u in dienst is radicaliseert. Het is belangrijk om vast te stellen of de radicalisering dermate ver is gevorderd dat het personeelslid ook terroristische activiteiten wil ondersteunen. Neem in zo'n geval contact op met de plaatselijke politie. Gezamenlijk kunt u de beste aanpak bespreken. U kunt een gesprek aangaan met het personeelslid of de persoon eventueel overplaatsen naar een ander bedrijfsonderdeel. Ook kan het voorkomen dat de politie vraagt niets te ondernemen in het belang van lopende onderzoeken. Het is niet nodig de plaatselijke politie te informeren als personeelsleden bijvoorbeeld strikter in hun geloof worden. Het gaat echt alleen om potentiële terroristen.

### **Nieuw personeel aannemen**

Bedrijven kunnen geradicaliseerde medewerkers aannemen die een terroristische aanslag willen plegen of ondersteunen, alhoewel de kans daarop klein is. Het is daarom belangrijk dat u aandacht besteedt aan de integriteit van de sollicitant.

De mogelijkheid om medewerkers door de AIVD te laten screenen is zeer beperkt. Meestal doet de dienst dat alleen voor vertrouwensfuncties bij bedrijven die behoren tot de vitale infrastructuur. Deze functies zijn erkend door een ministerie.

Een andere mogelijkheid is om een Verklaring omtrent Gedrag (VOG) van nieuwe medewerkers te vragen. Een onderdeel van Justitie, de dienst Justis, verleent een VOG als de kandidaat geen strafbare feiten of overtredingen heeft begaan. Het gaat

hierbij dan om strafbare feiten die een relatie met de uit te oefenen functie hebben. De dienst Justis heeft met diverse bedrijfssectoren voor die specifieke sector een profiel met bepaalde delicten opgesteld. Als een sollicitant één van de delicten heeft begaan, wordt geen VOG afgegeven. Door de relatie tussen de functie en het delict is het bereik van het VOG (bewust) beperkt. Voor meer informatie zie [www.justitie.nl](http://www.justitie.nl) U kunt zoeken op 'Justis' of 'Verklaring omtrent Gedrag'.

Als u meer wilt weten over de achtergrond van een sollicitant is de meest gangbare procedure het controleren van referenties en het spreken met vorige werkgevers. Vergeet niet dat met diploma's en getuigschriften makkelijk te knoeien is. Vraag dus altijd naar het origineel. Controleer de gegevens die u verstrekt worden. Het is ook verstandig om sollicitanten te vragen zich te legitimeren met een geldig legitimatiebewijs.

### **Inhuur van extern personeel**

Veel bedrijven hebben extern personeel over de vloer. Bijvoorbeeld van uitzendbureaus, onderhoud-, installatie-, schoonmaak-, catering- en beveiligingsbedrijven. Daarnaast huren bedrijven adviesbureaus in die bijvoorbeeld de beschikking kunnen krijgen over belangrijke bedrijfsinformatie. Inhuur kan risico's met zich meebrengen als bedrijven zich er van tevoren niet van vergewissen wie ze binnen halen.

U kunt ongewenst gedrag van extern personeel ontmoedigen of beperken met:

- een gedragscode;
- een geheimhoudingsverklaring;
- procedures en voorschriften voor kwetsbare handelingen;
- beperkte toegang tot informatie en gebieden binnen het bedrijf.

U kunt ook van de bedrijven die u inhuurt een Verklaring omtrent Gedrag van een rechtspersoon aanvragen. Met deze verklaring kunnen rechtspersonen hun integriteit tonen aan overheden, partners en bedrijven. De dienst Justis van Justitie geeft de Verklaring af. Voor meer informatie zie [www.justitie.nl](http://www.justitie.nl) U kunt zoeken op 'Justis' of 'Verklaring omtrent Gedrag'.

### **3.3 INFORMATIE**

Terroristen kunnen bedrijfsinformatie zoals persoonsgegevens of technische informatie misbruiken. Het is dan ook belangrijk dat u de aanwezige informatie, informatiedragers en informatiestromen inventariseert. Hieronder beschrijven we enkele mogelijkheden om bedrijfsinformatie te beschermen of effectief te vernietigen.

#### **Fysieke en procedurele maatregelen**

Als u beschikt over een inventarisatie van de informatie, de informatiedragers en de informatiestromen, kunt u beoordelen of uw personeel over alle informatie moet beschikken. Veel informatie wordt verleend op basis van het principe 'nice to know'. Als u kiest voor informatieverstrekking op basis van het principe 'need to know' kunt u gevoelige informatie voor bepaalde medewerkers afschermen. Een digitaal systeem met de mogelijkheid autorisatieniveaus en paswoorden in te stellen kan u hierbij helpen.

Met uw personeel kunt u procedures afspreken om te voorkomen dat informatie rondslingert. Denk bijvoorbeeld aan:

- afgesloten bureaus en kasten, uitgewiste whiteboards, afgesloten kamers en een schoon en leeg bureau (clean desk);
- schermbeveiliging gebruiken op computers en voorzichtig om gaan met paswoorden;
- spreek met uw medewerkers af dat zij in principe geen informatie mee naar huis nemen;
- laat documenten en laptops niet onbeheerd achter;
- verstrek niet zomaar belangrijke informatie via de telefoon of in de trein;
- berg vertrouwelijke en bedrijfsgevoelige documenten op in een inbraakwerende en/of brandwerende kast.

Om de naleving van afspraken te ondersteunen is het handig afspraken op papier te zetten en uw personeel eventueel een geheimhoudingsverklaring te laten ondertekenen.

#### **IT-beveiliging**

De beveiliging van IT wordt steeds belangrijker. Een goede beveiliging voorkomt economische schade en vermindert de kans dat terroristen informatie uit uw systemen gebruiken voor een aanslag. Terroristen krijgen steeds meer handigheid in het gebruik van ICT. Ze kunnen bedrijven lamleggen door binnen te dringen in een beveiligd computersysteem (hacken). Daarnaast kunnen ze kwaadwillige software toevoegen, functionaliteiten in- en uitschakelen of veranderen en bijvoorbeeld de samenstelling van producten op afstand wijzigen.

Schaf goede software van betrouwbare fabrikanten en leveranciers aan die bestand is tegen virusuitbraken en beschikt over een goede firewall. Van tijd tot tijd is het verstandig uw computersysteem te laten analyseren op risico's. Het coderen van bestanden en het werken met paswoorden kunnen bijdragen aan een betere IT-beveiliging. Daarnaast is het verstandig gebruik te maken van verschillende servers en regelmatig back-ups te maken. Besteed aandacht aan de betrouwbaarheid van het externe IT-personeel.

#### **Vernietigen informatie**

U kunt informatie vernietigen door het papier te verscheuren, te verbranden of te verpulveren. Ook zure of chemische technieken zijn voor dit doel geschikt. Maak de keuze tussen het (deels) zelf vernietigen van de informatie of het laten vernietigen. In het laatste geval is het verstandig goede afspraken met het vernietigingsbedrijf te maken. U moet er zeker van zijn dat het ingehuurde bedrijf zich aan de procedures houdt en de afgesproken norm haalt.

Let op: bij het vernietigen van informatie gaat het niet alleen om papieren informatie. Ook servers en computers moeten regelmatig geschoond worden.

Het vernietigen van beide soorten informatie kunt u niet alleen overlaten aan medewerkers die verantwoordelijk zijn voor het beheer van ICT of faciliteiten. Ook de beveiligingscoördinator speelt hierin een rol.

#### **4. PREPARATIEVE MAATREGELEN**

Preparatieve maatregelen hebben betrekking op het daadwerkelijk optreden door uw personeel bij een aanslag. Deze activiteiten zijn van voorbereidende aard. Preparatieve maatregelen voor een terroristische aanslag en een ramp komen grotendeels met elkaar overeen.

Het belangrijkste is dat u voorzieningen heeft om uw personeel in veiligheid te brengen als er een aanslag is gepleegd.

Voorbeelden van preparatieve maatregelen zijn:

- een ontruimingsplan opstellen;
- uw personeel informeren over het ontruimingsplan, de vluchtwegen en de ontruimingsprocedures;
- een plek aanwijzen waar medewerkers zich moeten verzamelen;
- mensen een opleiding voor bedrijfshulpverlening laten volgen;
- regelmatig ontruimingsoefeningen houden;
- regelmatig controleren of het waarschuwingssysteem werkt;
- regelmatig controleren of materiaal de vluchtwegen niet verspert;
- aangeven welke procedures medewerkers moeten volgen bij bommeldingen en verdachte pakketjes;
- veilige plekken binnen uw bedrijf aanwijzen als het niet verstandig is naar buiten te gaan. Bijvoorbeeld als er een aanslag plaatsvindt met chemische, biologische, radiologische en nucleaire wapens (CBRN-middelen);
- kijken of u uw airconditioning kunt uitzetten. Bijvoorbeeld in geval van een poederbrief of een aanslag met CBRN-middelen;
- zorgen voor voldoende middelen, zoals dekens.

Een belangrijk onderdeel van een ontruimingsplan is het hebben van juiste, actuele telefoonlijsten. Wie moeten wanneer gebeld worden bij een aanslag? Maak ook een lijst van telefoonnummers van hulpverleningsinstanties en de gemeente. Bij de plaatselijke politie en de overige lokale autoriteiten moet ook in ieder geval één contactpersoon van uw bedrijf bekend zijn.

Het ontruimingsplan besteedt ook aandacht aan ontruimingen in verband met een brand, het gebruik van CBRN-middelen (denk aan poederbrieven) en bommeldingen. Het is verstandig procedures vast te stellen voor het geval uw bedrijf of medewerkers geconfronteerd worden met een poederbrief of met een bommelding. Train medewerkers geregeld in het herkennen van en het reageren op verdachte brieven, pakketjes en bommeldingen.

Ook maatregelen die de bedrijfscontinuïteit verbeteren tijdens of na een aanslag behoren tot de preparatieve maatregelen. Voorbeelden hiervan zijn het maken van regelmatige back-ups van computerbestanden en ervoor zorgen dat belangrijke documenten ook elders elektronisch of fysiek beschikbaar zijn.

#### **5. RESPONSIEVE MAATREGELEN**

Responsieve maatregelen hebben te maken met het bestrijden van de aanslag, het beperken van de nadelige gevolgen ervan en het verlenen van hulp. Een ander woord voor respons is 'repressie'. De maatregelen in deze categorie zijn vooral toebedeeld aan de hulpverleningsorganisaties: brandweer, politie en ambulance. Het effect van de responsieve maatregelen is ook afhankelijk van de mate waarin een getroffen bedrijf zich voorbereid heeft op rampen en incidenten. Denk aan regelmatige oefening en een goede opleiding van het personeel.

Responsieve maatregelen tijdens een terroristische aanslag komen grotendeels overeen met de maatregelen tijdens een ramp of andere crisis. Toch zijn er ook verschillen. Dat is ook de reden dat de landelijke overheid in oktober 2006 is gestart met een landelijke campagne onder de titel 'Denk vooruit'. Deze campagne benadrukt dat elke crisis andere maatregelen verlangt. In de campagne staat centraal wat u kunt doen bij een grote brand, bij langdurige uitval van stroom, gas, water of telefoon, bij een overstroming, bij het vrijkomen van gevaarlijke stoffen en bij een terroristische aanslag.

Bij een terroristische aanslag is het van belang dat uw medewerkers alert zijn en informatie doorgeven aan de plaatselijke politie. Deze informatie kan helpen de daders op te sporen.

Op de website [www.crisis.nl](http://www.crisis.nl) vindt u de basale maatregelen voor de verschillende crises. Algemene informatie over crisismanagement en crisisbeheersing is te vinden op [www.veiligheid.minbzk.nl](http://www.veiligheid.minbzk.nl)

## **6. NAZORGSMAATREGELEN**

Nazorgsmaatregelen zijn activiteiten om de gevolgen van een aanslag te verhelpen en herhaling te voorkomen. Deze maatregelen zorgen voor een terugkeer naar de 'normale' situatie. Als u veel aandacht heeft besteed aan preparatieve maatregelen om de bedrijfscontinuïteit te bevorderen, komt dit de nazorg ten goede. Dat zou kunnen betekenen dat u heeft gezorgd voor een goede uitwijkmogelijkheid voor uw bedrijf als u niet meer in uw gebouw kunt werken. Ook kunt u maatregelen hebben genomen voor het behoud van informatie en gegevens. U heeft misschien uw servers ook buiten uw pand laten draaien en heeft voldoende back-ups gemaakt.

Uw personeel is waarschijnlijk voor u het belangrijkste. Het is dan ook aannemelijk dat u van tevoren goede verzekeringen heeft afgesloten, zodat uw werknemers niet de dupe van een aanslag op uw bedrijf worden (bijvoorbeeld door ziekte).

U kunt medewerkers ook psychische hulp aanbieden. Het is raadzaam met uw verzekeraar uw polis te bespreken om te kijken of u voldoende verzekerd bent.

