

# KAN UW BEDRIJF AANTREKkelijk ZIJN VOOR TERRORISTEN?

**Terroristen kunnen uitzijn op zo veel mogelijk slachtoffers of grote economische schade. Maar ook het zaaien van angst, onrust of het treffen van symbolische doelen kan het doel zijn. Wat kunt u doen om geen slachtoffer te worden of een bijdrage te leveren aan een aanslag? Analyseer uw situatie, beveilig uw organisatie en signaleer wat afwijkend is (ABS). Deze Checklist brengt u in twintig stappen dicht bij een veilige organisatie.**

## Analyseer

### **1. WEET WAT DE TERRORISTISCHE DREIGING IS. (A)**

Vier keer per jaar wordt het landelijke dreigingsniveau vastgesteld. Zijn er daarnaast alerteringen in één van de veertien sectoren die uw organisatie kunnen raken? Kijk op [www.nctb.nl](http://www.nctb.nl)

### **2. WERK SAMEN TEGEN TERRORISME EN CRIMINALITEIT. (A)**

De meest effectieve en kostenbesparende beveiliging ontstaat als u samenwerkt met uw omgeving: de politie, de sector en uw burens. Goed en geregeld contact onderhouden, kan al genoeg zijn.

### **3. MAAK ELK JAAR EEN RISICOANALYSE. (A)**

Wat zijn de risico's van uw organisatie? Probeer uw organisatie eens door de ogen van criminelen of terroristen te bekijken. Bedenk of uw bedrijf aantrekkelijk kan zijn voor terroristen. Denk niet alleen aan mogelijke slachtoffers en economische schade. Terroristen zijn vaak ook uit op symbolische doelen en het veroorzaken van angst en onrust. Weeg bestaande en nieuwe maatregelen af tegen de kosten en het effect.

### **4. STEL EEN VEILIGHEIDSPAN OP. (A)**

Denk na over de mogelijke risico's uw bedrijf loopt en hoe u daarmee omgaat. Beschrijf de procedures die uw bedrijf hanteert. Weten mensen in alle moeilijke situaties wat ze moeten doen en wordt uw plan door iedereen ondersteund?

### **5. ZORG VOOR GOEDE PROCEDURES VOOR CRISISSITUATIES. (A)**

Zorg dat er goed werkende procedures zijn voor allerlei soorten crisissituaties waarmee u te maken kunt krijgen. Waaronder ook bommeldingen, bedreigingen, bomaanslagen en verdachte pakketjes.

### **6. OEFEN UW VEILIGHEIDSPROCEDURES ELK JAAR. (A)**

Pas het veiligheidsplan en de procedures aan na elke oefening.

### **7. VERZEKER UW ORGANISATIE ALS DAT NODIG IS. (A)**

Terrorisme is in bijna alle polissen uitgesloten. Vergoeding kan alleen als dekking voor terrorisme in de polis van het bedrijf is opgenomen. Kijk op [www.terrorismeverzekerd.nl](http://www.terrorismeverzekerd.nl)

## Beveilig

### **8. BESCHERM PERSOONSgegevens EN KENNIS VAN UW BEDRIJF. (B)**

Kan uw informatie of kennis bijdragen aan een aanslag, als het in verkeerde handen zou vallen? Bescherm uw gegevens goed. Vernietig bedrijfsgevoelige informatie zodra u het niet meer nodig hebt.

### **9. BESCHERM UW MEDEWERKERS. (B)**

De veiligheid van uw werknemers is uw zorg. En dat stopt niet bij de poort. Ook het woon- werkverkeer van medewerkers, huisadressen en persoonlijke gegevens op internet kunnen medewerkers - en uw organisatie - kwetsbaar maken.

#### **10. ZORG VOOR EEN GOEDE BEVEILIGING VAN UW PAND. (B)**

Voorbeelden zijn goed hang- en sluitwerk, alarmsystemen, goede verlichting en video-observatie.

#### **11. WEET WIE IN UW ORGANISATIE AANWEZIG ZIJN. (B)**

Hebt u een helder toegangsbeleid en een goede toegangscontrole?

#### **12. ZORG VOOR ZICHTBAARHEID IN EN OM UW BEDRIJF. (B)**

Door de bedrijfsruimten en de omgeving schoon te houden, signaleert u eerder bijzonderheden.

Zorg dat schoonmaakmedewerkers weten welke zaken ze moeten melden.

#### **13. BEVEILIG GEVAARLIJKE STOFFEN. (B)**

Terrorisme stelt andere eisen aan de beveiliging van stoffen dan milieu-, ARBO-regelgeving of criminaliteitspreventie.

Hebt u (grote) voorraden Chemische, Biologische, Radioactieve en Nucleaire (CBRN) stoffen? Of stoffen waarmee explosieven gemaakt kunnen worden? Maak dan afspraken met de politie over incidentopvolging en over de beveiliging van deze stoffen.

### **Signaleer**

#### **14. BIEDT GEEN GELEGENHEID VOOR VOORBEREIDINGEN. (S)**

Terroristen die een aanslag voorbereiden, hebben allerlei zaken nodig. Denk aan de zes V's: valuta, verblijf, verkenningen, voorwerpen (o.a. grondstoffen), vervoer of valse documenten.

#### **15. ZORG DAT SIGNALLEN UIT UW ORGANISATIE WORDEN OPGEVANGEN EN VERWERKT. (S)**

Weten medewerkers die verdachte en ongebruikelijke omstandigheden signaleren waar ze die kunnen melden?

En weten ze wat er met hun signalen gebeurt? Hebt u een contactpersoon bij de politie?

#### **16. MAAK GEBRUIK VAN UW EIGEN KENNIS VAN UW ORGANISATIE. (S)**

Kijk goed naar uw eigen bedrijf. Leg verbanden aan in uw voorraad- of managementsystemen om ongebruikelijke situaties te ontdekken. Vertrouw op uw gevoel: als iets niet klopt, maak er dan melding van.

#### **17. WEET MET WIE U ZAKEN DOET. (S)**

Laat nieuwe contractanten zich legitimeren. Onderzoek de kredietwaardigheid van een nieuwe organisatie, of vraag naar een Verklaring omtrent het Gedrag van Rechtspersonen (VOGrp). Kijk op [www.justitie.nl](http://www.justitie.nl)

#### **18. TREK ALTIJD REFERENTIES NA BIJ NIEUW PERSONEEL. (S)**

Als u personeel inhuurt, werk uitsluitend met betrouwbare bedrijven. Maak afspraken over de toegang van hun personeel tot uw organisatie. Vraag externen die u inhuurt naar een Verklaring Omtrent het Gedrag (VOG). Kijk op [www.justitie.nl](http://www.justitie.nl)

#### **19. SIGNALEER EN GA HET GESPREK AAN MET PERSONEEL DAT ZICH EXTREEM, RADICAAL OF GEWELDDADIG UITLAAT. (S)**

Het kan een aanwijzing zijn dat mensen radicaliseren in hun denkbeelden. In sommige gevallen kunnen ze zelfs bereid zijn geweld toe te passen. Als u vermoedt dat een personeelslid gewelddadig radicaliseert, neemt u dan contact op met de politie.

#### **20. NEEM BIJ BEDREIGINGEN, AFPERSING OF ONTVOERING ALTIJD ONMIDDELIJK CONTACT OP MET DE POLITIE. (S)**

Als u spreekt met de bedreiger, luister goed, vraag door, maar ga niet onderhandelen.

Neem direct contact op met de politie. Doorbreek de situatie door hulp te zoeken.

