

**WAT KAN EEN
HRM-FUNCTIONARIS
ONDERNEMEN
TEGEN TERRORISME?**



HOE KUNT U TE MAKEN KRIJGEN

MET TERRORISME?

Terrorisme is geen onderwerp waarmee we dagelijks worden geconfronteerd. Toch kunnen bedrijven ermee te maken krijgen, ook u als HRM-functionaris. Terroristen kunnen uw bedrijfsgebouw als doelwit op het oog hebben. Of uw producten, diensten, kennis en informatie ontvreemden en misbruiken. Bovendien kunt u medewerkers in dienst hebben of nemen die bereid zijn om terroristische activiteiten te ondersteunen.

We kunnen nooit alle gevaren uitsluiten. Maar we kunnen wél proberen de risico's te verminderen. Dat vraagt om adequaat optreden van de overheid en van bedrijven. Ook u als HRM-functionaris kunt een rol spelen om te voorkomen dat uw bedrijf wordt misbruikt.

Zo kunt u als HRM-functionaris te maken krijgen met een terroristische dreiging:

- door de producten, diensten, kennis of informatie van uw bedrijf; soms kunt u - zonder dat te weten - beschikken over informatie of goederen die interessant kunnen zijn voor terroristen.
- door geradicaliseerd personeel in dienst te hebben / nemen: soms zijn er aanwijzingen dat medewerkers mogelijk bereid zijn terroristische activiteiten goed te keuren, te ondersteunen of uit te voeren.

- door inhuur van extern personeel: ook extern personeel kan een toekomstige terroristische dreiging vormen, bijvoorbeeld door zich informatie toe te eigenen en die aan terroristen te overhandigen.

Meer weten?

- Kijk op www.nederlandtegenterrorisme.nl/bedrijven.
- Bestel of download op deze site de Handreiking voor bedrijven. Wat kan uw bedrijf ondernemen tegen terrorisme?

WELKE MAATREGELEN KUNT U NEMEN?

U kunt veel doen om uw bedrijf tegen terroristische acties te beveiligen. Door het nemen van preventieve maatregelen kunt u proberen de directe oorzaken van onveiligheid te voorkomen. Hierdoor is uw bedrijf een minder makkelijk doelwit voor terroristen. Dat geldt des te meer wanneer u uw maatregelen richt op zowel de beveiliging van objecten (locaties), diensten en processen, als op personeel en informatie. Hieronder worden de maatregelen beschreven waar u als HRM-functionaris een rol in kunt spelen.

BEWUSTWORDING PERSONEEL

U kunt de bewustwording rond het belang van beveiliging vergroten door uw personeel aan te spreken op hun verantwoordelijkheid voor de beveiliging van het bedrijf. Dat kan tijdens functionerings- en beoordelingsgesprekken, maar ook tijdens een aparte themabijeenkomst.

Vraag aandacht voor:

- de wijze waarop uw bedrijf omgaat met risico's;
- de procedures binnen het bedrijf, zoals het afsluiten van kasten, clean desk, toegangscontrole, bezoekersregistratie ed.;
- de mogelijke sancties als personeel niet volgens de voorschriften handelt;
- de bewegingsvrijheid van medewerkers binnen het bedrijf (instelling van autorisatieniveaus);
- de beveiliging en afscherming van informatie, bijv. door het verstrekken van informatie op basis van het principe 'need to know' (invoeren autorisatieniveaus en paswoorden).

Om naleving van de gemaakte afspraken te ondersteunen, is het verstandig deze op papier te zetten, bijvoorbeeld in arbeidsvoorwaarden/reglementen of huisregels van uw bedrijf. U kunt ook een gedragscode opstellen of uw personeel een geheimhoudingsverklaring laten ondertekenen. Zorg bij alle maatregelen voor steun van de bedrijfsleiding.

Bij geradicaliseerd personeel kunt u contact opnemen met de plaatselijke politie. Gezamenlijk kunt u de beste aanpak bespreken.

NIEUW PERSONEEL AANNEMEN

Bedrijven kunnen medewerkers aannemen die een terroristische aanslag ondersteunen of wellicht zelfs willen plegen. Hoewel de kans klein is dat u juist een potentiële terrorist in dienst neemt, is het voor

de veiligheid van uw bedrijf altijd belangrijk dat u aandacht besteedt aan de integriteit van de sollicitant, bijvoorbeeld door:

- het natrekken van referenties en het spreken met vorige werkgevers;
- het controleren van diploma's en getuigschriften op echtheid (vraag om originelen);
- de sollicitanten te vragen zich te legitimeren met een geldig legitimatiebewijs.

Ook is het mogelijk om van nieuwe medewerkers een Verklaring omtrent Gedrag (VOG) te vragen. Justitie verleent een VOG als de kandidaat geen strafbare feiten of overtredingen heeft begaan die een relatie hebben met de uit te oefenen functie.

Voor meer informatie: www.justitie.nl.

INHUUR VAN EXTERN PERSONEEL

Mogelijk krijgt u ook extern personeel over de vloer, zoals van uitzendbureaus, adviesbureaus, onderhoud, installatie-, schoonmaak-, catering- en beveiligingsbedrijven. Inhuur kan risico's met zich meebrengen als u zich er van tevoren niet van vergewist wie u binnenhaalt. 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. Voor meer informatie: www.justitie.nl.

HERKENNEN VAN SIGNALLEN

Om signalen voor concrete dreiging op te merken, moet u weten wat verdachte of ongebruikelijke handelingen en situaties zijn. Deze passen niet in het normale plaatje. U maakt het voor uzelf makkelijker om afwijkingen te constateren als u heldere procedures heeft en deze naleeft. Het gaat om procedures over de omgang met (bedrijfs)informatie, of over de registratie van grondstoffen en middelen.

Signalen kunnen verdacht zijn omdat:

- de handeling die u signaleert, zelf verdacht is, zoals:
 - (digitale) pogingen om kennis, informatie en goederen te ontvreemden die geschikt zijn voor de voorbereiding van een aanslag;
- het tijdstip van de handeling verdacht is, zoals:
 - aanwezigheid van werknemer en gebruik van vertrouwelijke informatie ná sluitingstijd;
- de locatie waar de handeling plaatsvindt verdacht is, zoals:
 - aanwezigheid van werknemer op locatie waar werknemer niet hoeft te zijn.

dreiging vormen. Samen met leidinggevendend kunt u als HRM-functionaris alert zijn op dergelijke signalen. Het gaat om personen die al vergevorderd zijn in hun radicalisering en bereid zijn steun te verlenen aan terroristische aanslagen of zelfs bereid zijn deze uit te voeren. Hun aantal is beperkt. Of sprake is van geradicaliseerd personeel hangt af van een combinatie van factoren.

Dit zijn enkele signalen voor de aanwezigheid van geradicaliseerd personeel:

- het voorhanden hebben of opzoeken via internet van extremistische uitingen;
- het afgeven van goedkeurende signalen over terroristische aanslagen;
- het reizen naar regio's of landen met een terroristisch conflict of trainingskampen;
- een plotselinge afkeer hebben van 'westerse gewoonten' zoals gemengde activiteiten (man/vrouw) en het drinken van alcohol;
- het dragen van specifieke kleding en symbolen of een plotselinge verandering van kledinggedrag.

Het is mogelijk dat personeel dat al bij u in dienst is radicaliseert. Dit kan een toekomstige terroristische

CHECKLIST VOOR HRM-FUNCTIONARISSEN

1. Stel samen met de beveiligingscoördinator en / of de bedrijfsleiding, bijv. op basis van de Handreiking voor bedrijven, vast welke specifieke terroristische dreigingen en risico's op uw bedrijf kunnen afkomen.
2. Stel vast welke aanvullende beveiligingsmaatregelen gericht op het personeel de risico's effectief kunnen terugdringen. Maak een afweging tussen de kosten en de baten (effecten).
3. Neem de aanvullende beveiligingsmaatregelen op in de arbeidsvoorwaarden / reglementen of huisregels van uw bedrijf.
4. Stel - met de beveiligingscoördinator - vast of een toegangscontrole door tassencontrole of onderzoek aan kleding gewenst is. Zo ja, informeer het personeel hierover.
5. Stel - met de beveiligingscoördinator - vast of het wenselijk is medewerkers, bezoekers en extern personeel te beperken in hun bewegingsvrijheid. Zo ja, voer autorisatieniveaus in.
6. Stel - met de beveiligingscoördinator - vast of het wenselijk is medewerkers en extern personeel beperkt toegang te verlenen tot informatie en zo informatie te beveiligen. Zo ja, voer autorisatieniveaus en het gebruik van paswoorden in.
7. Informeer het personeel over de procedures binnen het bedrijf, zoals het afsluiten van kasten, clean desk, toegangscontrole en bezoekersregistratie. Oefen de procedures en beveiligingsmaatregelen.
8. Besteed aandacht aan veiligheid in aanstellings-, functionerings- en beoordelingsgesprekken.
9. Wijs medewerkers op hun verantwoordelijkheid ten aanzien van veiligheid. Organiseer eventueel een bijeenkomst over veiligheid en beveiliging.
10. Besteed bij de aanname van nieuw personeel aandacht aan de integriteit van de sollicitant. Controleer de referenties, vraag een Verklaring omtrent Gedrag (VOG) en vergeet niet diploma's, getuigschriften en identiteitsbewijzen op echtheid te controleren.
11. Zorg ervoor dat u te maken hebt met betrouwbare bedrijven als u extern personeel inhuurt. Vraag een Verklaring omtrent Gedrag van een rechtspersoon aan, en maak duidelijke afspraken met de externe partij.

