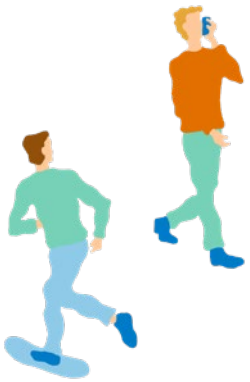
Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Veilig ondernemen op drukke plekken

Bent u voorbereid op een terroristische aanslag?

Veilig ondernemen op drukke plekken



Als onderneming of organisatie staat u midden in de samenleving. Zeker als u gevestigd bent op een plek waar grote groepen mensen zich regelmatig verzamelen. Samen kunnen we de veiligheid vergroten en schadelijke gevolgen beperken. Neemt u voldoende maatregelen tegen een terroristische aanslag? Toets de kwetsbaarheid van uw organisatie:

- Onze organisatie bevindt zich op een locatie waar **veel mensen** komen.
- Er worden **regelmatig evenementen** in onze directe omgeving of locatie georganiseerd.
- Onze locatie is **internationaal bekend** of heeft een **symbolische waarde** in Nederland.
- Onze locatie heeft een **open karakter**: makkelijk te betreden en/of met snelheid inrijdbaar.

Basisveiligheid

Is één van bovenstaande stellingen op u van toepassing? Bekijk dan ons dossier over basisveiligheid:

→ Maatregelen **Basisveiligheid**

Verhoogde kwetsbaarheid

Zijn er meerdere stellingen toepasbaar op uw onderneming of organisatie? Verdiep u dan in zowel de basisveiligheid als de verhoogde kwetsbaarheid.

→ Maatregelen **Verhoogde kwetsbaarheid**

Basisveiligheid

Uw onderneming is uniek. En de situatie is op iedere plek anders. Gebruik de voorbeelden en handvatten ter inspiratie. Kies de maatregelen die voor uw onderneming relevant zijn. Dit is aanvullend op de maatregelen die de overheid neemt om incidenten te voorkomen. Veel van de basismaatregelen die worden ingezet tegen criminaliteit kunnen ook effectief zijn tegen terrorisme.

Blijf op de hoogte van de algemene dreigingssituatie

Het is van belang om op de hoogte te blijven van de algemene dreigingssituatie in Nederland. De NCTV publiceert viermaal per jaar het Dreigingsbeeld Terrorisme Nederland (DTN).

Maak een risicoanalyse

Deze analyse maakt inzichtelijk welke risico's uw organisatie loopt, welke risico's acceptabel zijn en tegen welke risico's maatregelen nodig zijn. De risicoanalyse maakt de ernst van het effect van de meest waarschijnlijke acties van mensen die kwaad willen duidelijk, rekening houdend met de bestaande weerstand van de organisatie.

Dit kunt u zelf doen (bijvoorbeeld met behulp van het stappenplan in dit document). U kunt hier ook een beveiligingsbureau voor inschakelen. Suggesties voor Technische beveiligingsbedrijven kunt u vinden via het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Particuliere beveiligingsbedrijven met een vergunning van de minister van Justitie en Veiligheid zoals bedoeld in de Wet particuliere beveiligingsorganisaties en recherchebureaus kunt u bijvoorbeeld vinden via de websites van diverse brancheorganisaties.

Alertheid op verdachte objecten, personen of transacties

Het is van belang de mogelijk verdachte situatie steeds af te zetten tegen de normale situatie en de context te bekijken. Situaties kunnen 'verdacht' zijn omdat:

- de handeling die gesignaleerd is, zelf verdacht is
  Bijvoorbeeld: ongebruikelijke interesse in het bedrijf, filmen/fotograferen van de beveiliging van de onderneming, personen die hun identiteit verhullen en diefstal van bedrijfskleding, -legitimatiebewijzen of -eigendommen.
- het tijdstip van de handeling verdacht is
  Bijvoorbeeld: incidenten na sluitingstijd en terugkerende handelingen.
- de locatie waar de handeling plaatsvindt verdacht is
  Bijvoorbeeld: omdat daar informatie of middelen te vinden zijn die gebruikt kunnen worden bij een aanslag.

Op de website veiligondernemenbeginthier.nl zijn voorbeelden van trainingen te vinden op het gebied van criminaliteit die een bijdrage leveren bij het creëren van bewustzijn bij uw personeel, bijvoorbeeld de 360 graden veiligheidstraining.

Bij mogelijke verdachte handelingen is contact met de lokale politie aan te raden. Mogelijk heeft u specifieke afspraken met de politie over waar u terecht kunt met uw zorgen. Als dat niet het geval is kunt u contact opnemen met 0900-8844 (geen spoed) of 112 (spoed, bijvoorbeeld in geval van levensbedreigende situaties of een misdrijf).

Wilt u meer weten over verdachte transacties? Bezoek de website van Financial Intelligence Unit (FIU) Nederland. Daar ziet u onder andere welke transacties u moet melden.

Nette en overzichtelijke omgeving

Houd uw gebouw en omgeving zo schoon en overzichtelijk mogelijk. In een nette omgeving vallen afwijkende en verdachte situaties eerder op.

Signaleren en melden van radicalisering

U kunt hierbij denken aan het creëren van een interne procedure voor het melden van (vermoedens van) radicalisering. Mocht u (of een van uw medewerkers) het vermoeden hebben dat iemand in uw omgeving radicaliseert, dan vindt u op de website van de Rijksoverheid meer informatie, onder andere over waar u terecht kunt met vragen en zorgen.

Werk samen met andere ondernemers

Met naburige ondernemers kunt u afspraken maken over het elkaar informeren over incidenten, het gezamenlijk inhuren van beveiligingspersoneel of het bespreken van verdachte of risicovolle situaties in de afzonderlijke ondernemingen en de publieke ruimte.

Er zijn verschillende mogelijkheden om dit te faciliteren, maar u kunt hierbij denken aan een:

- Gezamenlijk Keurmerk Veilig Ondernemen
- Structureel veiligheidsoverleg
- App- of SMS-groep met het thema 'veiligheid'
- Gezamenlijk online platform (bijvoorbeeld chainels)
- Gezamenlijke Bedrijven Investeringszone (BIZ)
- Stichting collectieve beveiliging oprichten
- Aansluiten bij aanpak Veilig Uitgaan (meer info via het CCV).

Bedrijfshulpverlening op orde

Zorg voor een bevoegd bedrijfshulpverlener in uw onderneming, net als een BHV-plan, trainingen en oefeningen conform de geldende standaard. U kunt hierbij denken aan: vluchtroutes, bewegwijzering en werkende brandblussers. Zie voor algemene informatie over bedrijfshulpverlening het Arboportaal.

Maak een ontruimingsplan

Maak een ontruimingsplan voor uw organisatie.
In de 'Handreiking Bedrijfshulpverlening' [SMNm-B1] van Stichting van de Arbeid staat hier meer informatie over. Hierin vindt u een voorbeeld inhoudsopgave van een BHV-plan. Bedenk hierbij dat het in geval van een aanslag mogelijk nodig is af te wijken van het reguliere ontruimingsplan.

Fysieke beveiliging

Fysieke beveiligingsmaatregelen zijn onder meer: inzet van particulier beveiligingspersoneel, slagwerende beglazing, hekwerk, goed hang- en sluitwerk, juiste verlichting en beveiliging van deuren en ramen.

Zie voor meer tips op het gebied van veilig ondernemen (zoals inbraak- en overvalpreventie, brandveiligheid en tegengaan agressie en geweld) de website 'Veilig ondernemen begint hier' van het CCV. Hier vindt u onder andere een scan over veilig ondernemen en contactgegevens van beveiligingsbedrijven in uw regio.

Huisregels opstellen

Iedere winkel mag binnen de grenzen van de wet zijn eigen regels bepalen, denk bijvoorbeeld aan het meenemen van tassen. Het is in dat geval wel nodig huisregels te hebben en dit daarin te vermelden.

Huisregels hebben een preventieve werking. Het vooraf verlenen van toestemming voor tassencontrole, verplicht gebruik van een winkelwagentje of -mandje, het beperken van de toegang van (hinderlijke) groepen; het mag allemaal en klanten mogen erop aangesproken worden. Voorwaarde is wel dat de huisregels duidelijk zichtbaar zijn bij de ingang van de winkel. Een klant die de winkel betreedt, accepteert stilzwijgend de voorwaarden.

Op de website 'Veilig ondernemen begint hier' vindt u voorbeeld-huisregels. Ook hebben veel brancheorganisaties voorbeeld-huisregels die u kan overnemen of bestellen.

Toegangs- en ontvangstbeleid

Denk bijvoorbeeld aan:

- Heldere scheiding tussen publieke en niet-publieke ruimtes
- Personeel herkenbaar d.m.v. naamplaatjes en/of uniform
- Aanspreken onbekende en onherkenbare personen in de niet-publieke ruimtes
- Receptie of gastheer/vrouw
- Uitdelen bezoekerspassen en de verplichting deze te dragen (denk ook aan het innemen)

Inventariseer ook locaties zoals technische ruimten en magazijnen en neem deze op in het toegangsbeleid.

Overweeg:

- Toegangscontrole
- Zonering
- Sleutelplan en sleutelbeheer
- Autorisatie van personeel tot bepaalde bedrijfsonderdelen en -systemen

Installeer verschillende veiligheidssystemen

Om de veiligheid van uw onderneming en de nabije omgeving te vergroten kunnen veiligheidssystemen zoals camerabeveiliging en alarmsystemen een bijdrage leveren. Voor onder andere een afwegingskader, kunt u de website van het CCV bezoeken. Ook kunt u kiezen een particuliere alarmcentrale in de arm te nemen. Dit zijn bedrijven waar alarmsignalen binnenkomen van elektronische alarmsystemen, en die ervoor moeten zorgen dat op een alarm-signaal actie wordt ondernomen.

U kunt uw camera's ook aanmelden bij de politie. Hierdoor heeft de politie overzicht van waar camera's hangen zodat zij in het geval van criminaliteit deze beelden kunnen opvragen.

Informatie- en cyberbeveiliging

Naast maatregelen om uw pand en personeel te beschermen is het ook van belang om uw informatie zo veilig mogelijk te houden. Denk hierbij bijvoorbeeld aan:

- bewustwording creëren bij uw personeel (ten aanzien van delen en bewaren van informatie)
- regelmatig back-ups maken
- wachtwoorden regelmatig updaten
- een kluis voor het bewaren van uw niet-digitale informatie
- veilig internet gebruik

Cybercriminaliteit omvat alle vormen van criminaliteit op het internet. Dit varieert van de verspreiding van computervirussen tot misbruik van persoonsgegevens. Cybercriminaliteit tegen het bedrijfsleven richt zich meestal op het verkrijgen van toegang tot kapitaal. Ook kunnen cybercriminelen er op uit zijn om bedrijfs- en productieprocessen te verstoren. Op 'Veilig Ondernemen begint hier' vindt u maatregelen die u kunt treffen om cybercriminaliteit tegen te gaan.

Bestaande sectorspecifieke veiligheidsmaatregelen

Voor bepaalde sectoren zijn er specifieke veiligheidsmaatregelen noodzakelijk, zoals overvalpreventie of crowd control. Op de website 'Veilig ondernemen begint hier' van het CCV vindt u hier meer informatie over.

Verhoogde kwetsbaarheid

In sommige gevallen is het nodig of wenselijk om naast de basismaatregelen nog extra maatregelen te nemen ter voorkoming van een aanslag.

Maak een specifieke risicoanalyse met het oog op een terroristische aanslag

Deze analyse maakt meer tot in detail inzichtelijk welke risico's de organisatie loopt met het oog op een terroristische aanslag, welke risico's acceptabel zijn en tegen welke risico's maatregelen nodig zijn. De gespecificeerde risicoanalyse maakt de ernst van het effect van de meest waarschijnlijke acties van mensen die kwaad willen duidelijk, rekening houdend met de bestaande weerstand van de organisatie.

Dit kunt u zelf doen (bijvoorbeeld met behulp van het bijgevoegde stappenplan) en u kunt hier ook een beveiligingsbureau voor inschakelen. Technische beveiligingsbedrijven kunt u bijvoorbeeld vinden via het CCV. Particuliere beveiligingsbedrijven met een vergunning van de minister van Justitie en Veiligheid zoals bedoeld in de Wet particuliere beveiligingsorganisaties en recherchebureaus kunt u bijvoorbeeld vinden via de websites van diverse brancheorganisaties.

Goed zicht en toezicht

Maak bewuste keuzes in de inrichting van uw onderneming, organisatie en openbare ruimte waarin deze zich bevindt. Zorg voor goed zicht én toezicht. U kunt hierbij denken aan:

- Het gebruik van doorzichtige vuilniszakken
- Regelmatig legen van vuilnisbakken
- De omgeving regelmatig inspecteren, zodat onregelmatigheden opvallen
- Goede verlichting in en rondom onderneming
- Ongebruikte ruimtes op slot doen

Maak bewuste keuzes in personeelsbeleid

Het is van belang om bewuste keuzes te maken in het personeelsbeleid, bijvoorbeeld via achtergrondchecks of screenings. U kunt bijvoorbeeld identiteitsbewijzen en diploma's controleren, referenties checken, verklaringen omtrent gedrag laten opvragen en gebruik maken van het waarschuwingsregister of een particulier onderzoeksbureau met een vergunning op basis van de Wet particuliere beveiligingsorganisaties en recherchebureaus met een keurmerk. Dit kan ook gelden voor tijdelijk personeel of onderaannemers. Houd deze checks ook actueel door ze geregeld uit te voeren.

Nauwere samenwerking met ondernemers in de buurt

Met naburige ondernemers of organisaties kunt u nauw gaan samenwerken. U kunt hierbij denken aan het aanstellen van een gezamenlijke *security manager* en het structureel spreken van politie en/of gemeente over het thema veiligheid.

Andere opties zijn het oprichten van een Bedrijven Investeringszone (BIZ) of organiseren van gezamenlijke trainingen voor het personeel op het vlak van *security awareness* of herkennen van afwijkend gedrag.

Afspraken over waarschuwen in geval van een acute verdachte situatie

Maak afspraken met andere ondernemers of organisaties in de nabije omgeving om elkaar te waarschuwen in het geval van een acute verdachte situatie. Dit kunt u doen door middel van een alarmerings-app, SMS groep of een facilitair intranet met een rode knop-functie (bijvoorbeeld via *chainels*).

Cameratoepassingen aangepast op specifieke punten en posities

U kunt bijvoorbeeld gebruik maken van verlichting en camera's met een bewegingssensor.

U kunt uw camera's ook aanmelden bij de politie. Hierdoor heeft de politie overzicht van waar camera's hangen zodat zij in het geval van criminaliteit deze beelden kunnen opvragen.

Het reguleren van en toezichthouden op vervoersbewegingen

Dit houdt in ieder geval in dat u toegangs- en ontvangstbeleid heeft (zie basisniveau). Denk hierbij ook aan de volgende maatregelen:

- Cameratoezicht
- Venstertijden
- Zo min mogelijk partijen toegang geven tot het gebied (dus bijvoorbeeld: gezamenlijk met naburige ondernemers schoonmaak/beveiliging etc. inhuren)
- Parkeerfaciliteiten personeel op enige afstand
- Toegangscontrole voertuigen door middel van het invoeren van bijvoorbeeld een passysteem

Nadenken en trainen personeel over beleid ten aanzien van ontruimen, schuilen en lockdown

Op voorhand valt er geen eenduidig advies te geven over wel of niet te ontruimen of de deuren van het gebouw te sluiten en op slot te doen ('*lockdown*'). Dit is afhankelijk van de situatie en de aard van het object. In het algemeen geldt:

- Een ontruiming vindt plaats als de politie dit aangeeft en/of als de dreiging reëel is en het aannemelijk is dat de situatie dusdanig is dat ontruimen van het gebouw het middel is om de aanwezige mensen in relatieve veiligheid stellen.
- Een gedeeltelijke ontruiming vindt plaats als het niet mogelijk is om de grote hoeveelheid mensen in één keer te evacueren.
- Schuilen op een veilige plek in het gebouw kan worden gekozen, bijvoorbeeld wanneer de dreiging vlak buiten het gebouw is of wanneer de exacte locatie van de dreiging nog onbekend is.
- Een lockdown (deuren dicht en op slot) vindt plaats als het niet mogelijk is een aanslag te voorkomen of te stoppen en de aanslagpleger(s) zich wel in hoog tempo verplaatst (/verplaatsen).
- De optie om 'niets te doen' ligt voor de hand als de politie vaststelt dat de dreiging niet reëel is.

Volg altijd de instructies van de politie.

Op de website crisis.nl vindt u meer informatie over wat u kunt doen bij een terroristische aanslag.

Specifieke voorbereidingen ten aanzien van ontruimen, schuilen en lockdown

U kunt hierbij denken aan het toevoegen en uitwerken van de scenario's schuilen en lockdown (zie hierboven) aan uw bestaande ontruimingsplan en het beschikbaar hebben van een '*saferoom*', een veilige plek in het gebouw om te kunnen schuilen. Tips voor het selecteren van een dergelijke ruimte:

- Ruimtes die omgeven zijn door muren, bij voorkeur met deuren die naar binnen open gaan.
- Indien een gebouw meerdere verdiepingen heeft: bij voorkeur niet op de begane grond of de eerste verdieping en in het midden van het gebouw.
- Niet in de buurt van trappen of liftschachten als deze een open verbinding hebben met de begane grond. Als deze ruimtes afgesloten zijn, zijn deze mogelijk juist geschikt.
- Er moet genoeg ruimte zijn om met meerdere mensen enige tijd te kunnen verblijven.
- Beoefen met uw personeel de gemaakte afspraken en maatregelen, bijvoorbeeld door het ontruimingsplan te oefenen.

Voorbereiden voor wat te doen na een aanslag

Maak een plan voor uw personeel met duidelijke instructies en afspraken over wat te doen na een aanslag. Hierbij kunt u denken aan:

- De toegankelijkheid van het gebied, want deze is mogelijk anders dan u gewend bent
- Mogelijk (tijdelijk) extra beveiliging
- Zorgdragen voor continuïteit eigen dienstverlening
- Rekening houden met de mogelijkheid van mensen die vluchten en gewonden die verzorgd moeten worden
- Ruimte bieden aan rouw en herdenken
- Traumaverwerking personeel
- Herstellen van vertrouwen

Voor meer informatie over slachtofferhulp, kunt u de websites van Slachtofferhulp Nederland en het IVP (expert bij schokkende gebeurtenissen) bezoeken.

Kwetsbaar voor inrijden door voertuigen

Mogelijk is uw onderneming kwetsbaar voor het inrijden door voertuigen. Of dit het geval hangt af van een tweetal factoren: de kwetsbaarheid van uw locatie of omgeving als doelwit voor een aanslag (internationaal bekend, symbolische plek, veel mensen bijeen etc), en de mate waarin uw locatie te bereiken is door een voertuig (open aanrijroute, kwetsbare gevel etc).

Zorg in dit geval voor toegangsbeleid en eventuele controle van de voertuigen, bijvoorbeeld door venstertijden in te stellen of cameratoezicht bij dynamische objecten.

In het geval van wachtrijen: probeer deze te voorkomen en te beperken, bijvoorbeeld door ruimte te bieden binnen in plaats van buiten. Verder kunt u fysieke beveiligingsmaatregelen nemen tegen inrijden of om te voorkomen dat er snelheid kan worden gemaakt, bijvoorbeeld door te werken met een speciaal type glas.

Hoe maak ik een risicoanalyse en een veiligheidsplan?

Grote kans dat u al hebt nagedacht over het tegengaan van bedrijfsongevallen en criminaliteit, en al passende voorzorgsmaatregelen heeft getroffen. U kunt hier met een risicoanalyse op verder bouwen.

De uitvoering van een risicoanalyse kan op verschillende manieren. Het is mogelijk om het zelfstandig te doen of een gespecialiseerd adviesbureau of beveiligingsbedrijf in te schakelen. Dit stappenplan ondersteunt bij het maken van een minder omvangrijke risicoanalyse en veiligheidsplan.

Het inschakelen van een adviesbureau is met name van belang als u veel risico denkt te lopen. Ook kunt u met bedrijven uit dezelfde branche, omgeving of uw ondernemersvereniging een gezamenlijke analyse (laten) uitvoeren.

Stap 1: identificeer het risico

Stel uzelf de volgende vragen:

- Wat kan worden geleerd van de overheid en media over het huidige veiligheidsklimaat in Nederland (en in de rest van de wereld) of over recente terroristische activiteiten?
  Zie voor achtergrondinformatie bijvoorbeeld www.nctv.nl en www.aivd.nl.
- Wat kan de lokale politie of gemeente u vertellen over criminaliteit en andere problemen in uw omgeving? Mogelijk heeft u al contact met politie in uw buurt. Zo niet, dan is de wijkagent een goede ingang.
- Is er iets met de locatie van uw bedrijf, uw bezoekers, gebruikers en personeel, uw activiteiten, waardoor u mogelijk kwetsbaar bent voor een aanslag?
  - Onze organisatie bevindt zich op een locatie waar **veel mensen** komen (op voorspelbare momenten).
  - Onze locatie is **internationaal bekend** of heeft een **symbolische waarde** in Nederland.
  - Er worden regelmatig **evenementen in onze directe omgeving** georganiseerd.
  - Onze locatie is **kwetsbaar voor voertuigen**.
- Houdt uw onderneming verband met prominente personen of organisaties die mogelijk terroristische doelen zijn?
- Zitten er organisaties of ondernemingen in uw omgeving die mogelijk kwetsbaar zijn voor een aanslag (waardoor u dat ook bent)?
- Zijn er aspecten van uw bedrijf of activiteiten (of die van uw personeel) die terroristen zouden willen gebruiken om een aanslag mee te plegen; zoals het maken van plattegronden, stoffen die ook kunnen worden gebruikt in explosieven of technische expertise?
- Is er online gevoelige informatie te vinden over uw onderneming (bijvoorbeeld foto's of plattegronden)? Is het mogelijk dat personen of andere bedrijven deze informatie over u publiceren?

Stap 2: bepaal wat u wil beschermen en identificeer uw kwetsbaarheden

Na het bepalen van de risico's, kunt u identificeren wat u wil beschermen. Uw prioriteiten voor bescherming zijn te verdelen in de volgende categorieën:

- **mensen** - bijvoorbeeld personeel, bezoekers, klanten en contractanten
- **activa** - bijvoorbeeld gebouw(en), bepaalde ruimtes in uw gebouw (zoals magazijnen of technische ruimtes), meubilair, uitrusting, plannen en gevoelige materialen
- **informatie** - bijvoorbeeld elektronische en papieren gegevens
- **processen en beleid** (het feitelijke operationele proces en essentiële diensten die nodig zijn om het te ondersteunen) - bijvoorbeeld supply chain en kritische procedures

Voor elke categorie overweegt u, met de kennis die u heeft vergaard in stap 1:

- **Wat is de kwetsbaarheid?** Bijvoorbeeld: het is een plek waar veel mensen bij elkaar komen (uw hal of ontvangstruimtes)
- **Waarom is het kwetsbaar?** Bijvoorbeeld: er staat veel meubilair in die hal waardoor er geen goed overzicht is en er zijn verschillende toegangswegen
- **Waar is het kwetsbaar voor?** Bijvoorbeeld: voor zakkenrollers. Mogelijk ziet u door de conclusies die u heeft getrokken in stap 1 dat deze ruimte ook kwetsbaar is voor terroristen die een aanslag willen plegen met explosieven of een mes.

U weet wat belangrijk is voor u en uw bedrijf. Het kan iets tastbaars zijn, bijvoorbeeld de kassa's en uw gebouw, maar ook uw IT-systeem of een apparaat dat essentieel is om het bedrijf te laten functioneren.

Stap 3: bepaal maatregelen om het risico te verminderen

Nu u heeft bepaald wat u wilt beschermen en waarom, kunt u bekijken welke maatregelen uw onderneming al heeft, hoe effectief ze zijn en waar de kwetsbaarheden zijn.

Onthoud, terrorisme is een misdaad. Veel van de voorzorgsmaatregelen die worden gebruikt om veilig en gezond te werken (in het kader van arbo wetgeving) en om criminelen af te schrikken zijn ook effectief tegen terroristen. Dus voordat u investeert in aanvullende veiligheidsmaatregelen, bekijk goed wat u al doet.

Mogelijk heeft u al passende voorzorgsmaatregelen getroffen en een goede veiligheidscultuur. In bovengenoemd voorbeeld komt u wellicht tot de conclusie dat de toegangswegen die op slot kunnen, dat ook zijn, dat u al bekwaam beveiligingspersoneel in dienst heeft en dat u een adequaat camera systeem heeft.

Mogelijk komt uit stap 1 en 2 naar voren dat u kwetsbaarheden heeft die nog níet (voldoende) beschermd zijn. Dan zijn aanvullende voorzorgsmaatregelen wenselijk.

Tips:

- Bekijk uw beveiliging altijd als totaalpakket. Denk na over fysieke beveiliging, cyberveiligheid, informatieveiligheid én persoonlijke veiligheid. Het heeft weinig zin te investeren in kostbare beveiligingsmaatregelen als ze gemakkelijk kunnen worden ondermijnd door een ontevreden personeelslid of leverancier vanwege onzorgvuldige werving of inkoopmethodes.
- Maak aanvullende maatregelen (waar mogelijk) rendabel door een zorgvuldige planning.
  - Introduceer nieuwe apparatuur of procedures in combinatie met bouwwerkzaamheden.
  - Probeer met naburige ondernemers afspraken te maken over gemeenschappelijke beveiligingsmaatregelen.
- Herstel (indien nodig) de beveiligingspraktijk. Het regelmatig beoordelen brengt voordelen tegen minimale kosten. Want medewerkers zijn mogelijk niet op de hoogte van bestaande beveiligingsmaatregelen of er zijn gewoonten ontstaan om ze te omzeilen (zoals 'handige' looproutes door nooduitgangen).

Stap 4: maak een veiligheidsplan

Een veiligheidsplan bevat een overzicht van alle genomen beveiligingsmaatregelen en wat deze moeten beschermen. Effectieve beveiligingsplannen zijn eenvoudig, duidelijk en flexibel. Meestal bevatten ze twee dimensies:

- **Beschermend** – een overzicht van inzet van alarmsystemen en beveiligingspersoneel, inzet van camera's, training van personeel, meldplicht etc.

- **Reactief** – een overzicht van de acties die het personeel moet uitvoeren bijvoorbeeld als ze een persoon zien die zich verdacht gedraagt, wat te doen als er een bommelding komt en een plan voor ontruiming, schuilen en lockdown.

Stap 5: controleer uw beveiligingsmaatregelen, train personeel, beoefen en test beveiligingsplannen

U moet uw plannen regelmatig herzien en beoefenen om ervoor te zorgen dat ze volledig, werkbaar en up-to-date blijven. Als er ergens anders een aanslag plaatsvindt, een verandering in dreiging of omstandigheden (bijvoorbeeld verbouwing in uw gebouw) is, is het raadzaam om te overwegen of uw plannen vernieuwd moeten worden.

Tips:

- Zorg er door training voor dat uw personeel hun verantwoordelijkheden begrijpt en de noodzaak van veiligheidsmaatregelen accepteert. Het is belangrijk dat beveiliging wordt gezien als onderdeel van ieders verantwoordelijkheid, niet alleen iets voor beveiligingsdeskundigen of -professionals.
  - Op de website veiligondernemenbeginthier.nl staan voorbeelden van trainingen op het gebied van criminaliteit, zoals de 360 graden veiligheidstraining.
- Maak het eenvoudig voor mensen om hun zorgen te delen of verdachte situaties te melden.
- Het verdient de aanbeveling om oefeningen samen met naburige ondernemers, politie en hulpdiensten en lokale autoriteiten uit te voeren.

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minvenj.nl
@nctv_nl

April 2018