Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Wat leveren extra maatregelen mijn organisatie op?

Terrorisme is één van de risico's waar uw organisatie mee te maken kan krijgen. Zeker wanneer u werkt met chemische, biologische, radiologische of nucleaire (CBRN) stoffen of kennis in huis heeft over deze stoffen.

CBRN-stoffen zijn voor kwaadwillenden namelijk interessante middelen om een aanslag mee te plegen. Een grote CBRN-aanslag is niet waarschijnlijk, maar ook een weinig effectieve aanslag met bijvoorbeeld een poederbrief of een giftige stof kan leiden tot grote maatschappelijke onrust.

Net als bij andere risico's die zich kunnen voordoen, zoals criminaliteit, bent u zelf verantwoordelijk voor de beveiliging van deze stoffen tegen diefstal of een aanslag. Veel organisaties hebben al een beveiligingsbeleid en hebben al bepaalde beveiligingsmaatregelen genomen. Met instrumenten zoals de Zelfanalysemodule CBRN Security kunt u inschatten of uw huidige maatregelen de risico's afdoende afdekken of dat aanvullende maatregelen nodig zijn.

Zeven redenen om extra beveiligingsmaatregelen te nemen

Beveiliging van uw CBRN-stoffen draagt bij aan het voorkomen van terroristische aanslagen in Nederland, maar extra beveiligingsmaatregelen brengen ook andere voordelen met zich mee.

1. Voorkomen van een terroristische aanslag
Goede beveiliging maakt het moeilijker voor kwaadwillenden om aan CBRN-stoffen te komen en dwingt hen om hun plannen aan te passen. Hierdoor neemt de blootstelling van potentiële daders toe, waardoor ook de kans op signalering, interventie en veroordeling toeneemt.

2. Investeren in beveiliging en veiligheid van de organisatie als geheel
Extra beveiligingsmaatregelen helpen criminaliteit te beperken. Daarnaast dragen beveiligingsmaatregelen zoals toegangsbeveiliging, zonering van activiteiten en het beoefenen van beveiligingsincidenten bij aan de veiligheid (safety) binnen de organisatie.

3. Aanzet tot efficiënter werken
Nadenken over beveiliging is vaak een aanzet tot organisatorische of informatietechnische maatregelen die kunnen leiden tot efficiënter werken.

4. Waarborgen van de bedrijfscontinuïteit en voorkomen van economische schade
Extra maatregelen, zoals het goed beveiligen van ICT-systemen en het ergens anders bewaren van back-up bestanden, zorgen ervoor dat de organisatie na een (moedwillig of ander) incident snel weer kan overgaan tot de normale gang van zaken.

5. Verbeteren van het imago van de organisatie
Klanten doen sneller zaken met organisaties als ze weten dat hun goederen daar veilig zijn. Aandacht voor terrorismebestrijding kan ook het internationale imago van het hele Nederlandse bedrijfsleven en de onderzoekssector versterken. En dit is weer goed voor de concurrentiepositie van individuele organisaties.

6. Voldoen aan (wettelijke) verplichtingen
Met extra beveiligingsmaatregelen voldoen organisaties eerder aan eisen die overheden of bijvoorbeeld toeleveranciers stellen. Dat kan onder andere een beperktere - en dus snellere - controle op de lading opleveren.

7. Beter contact tussen overheden en bedrijven
Als organisaties verdachte zaken melden bij de plaatselijke politie, ontstaat een beter beeld van dreigingen. De lokale autoriteiten kunnen daardoor gerichter informeren en eventueel organisatiespecifieke afspraken maken.

Investeer gericht

Een nuance is hier op zijn plaats. Niet alle deze redenen gelden voor alle organisaties. En we moeten realistisch blijven: Nederland is een open maatschappij, we kunnen niet alle gevaren uitsluiten. Bovendien brengen aanvullende maatregelen kosten met zich mee. Organisaties betalen zelf deze kosten. Het is goed altijd te (laten) beoordelen of extra maatregelen echt bijdragen aan het beperken van de kans op diefstal of een aanslag. U kunt de Zelfanalysemodule CBRN Security gebruiken om gericht te kijken of aanvullende maatregelen geboden zijn.

Dit factsheet is een uitgave van:
Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
www.nctv.nl
Maart 2013 | Publicatie-nr. J-8388