

HOE BEPAAL IK HET RISICO DAT MIJN BEDRIJF LOOPT?

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 4. De handreiking kunt u downloaden of bestellen op www.nederlandtegenterrorisme.nl/bedrijven

Risicoanalyse

Om een goede keuze uit alle mogelijke beveiligingsmaatregelen te maken om uw bedrijf tegen terroristische acties te beveiligen, is het verstandig eerst een risicoanalyse en een kosten-batenanalyse uit te voeren. In welke mate is er sprake van een terroristische dreiging in Nederland? Wat is het effect van een aanslag op de bedrijfsprocessen? En hoe kwetsbaar is het bedrijf voor terroristische activiteiten?

Een risico-analyse bestaat uit een afhankelijkheidsanalyse (analyse van cruciale belangen en afhankelijkheden, een dreigingsanalyse (kans op een terroristische) dreiging) en een kwetsbaarheidsanalyse (analyse van de weerbaarheid tegen specifieke dreigingen of activiteiten).

In een risicoanalyse wordt de kans op een terroristische aanslag ook gerelateerd aan de schade die daaruit kan voortkomen. Oftewel: **risico = kans x effect**.

De uitkomst van een risicoanalyse is dus de inschatting van de ernst van de schade die terroristische incidenten ondanks de weerbaarheid van een bedrijf veroorzaken.

In de kosten- en batenanalyse bekijkt u of de kosten van de extra maatregelen opwegen tegen de verwachte effecten. Op basis hiervan bepaalt u zelf welke aanvullende maatregelen u neemt.

1. METHODIEK RISICOANALYSE

Mensen en organisaties zijn voortdurend bezig dagelijkse risico's te beheersen. Vaak gebeurt dat intuïtief, zonder een expliciete aanpak of methodiek. Maar er zijn ook bedrijfssectoren en vakgebieden die gespecialiseerd zijn in het analyseren en managen van risico's. Een voorbeeld hiervan is de financiële sector, die zich bezighoudt met het beperken van risico's rond investeringen, verzekeringen en beleggingen. En de chemische industrie doet dat met ongevalrisico's.

Een ander soort risicomangement is het beperken van risico's die kwaadwillende personen, zoals terroristen, bewust veroorzaken. Hiervoor zijn specifieke risicoanalysemethoden ontwikkeld. Ze bestaan meestal uit een combinatie van een afhankelijkheidsanalyse, een dreigingsanalyse en een kwetsbaarheidsanalyse.

In de afhankelijkheidsanalyse staan de kroonjuwelen van het bedrijf centraal: vitale bedrijfsprocessen en cruciale onderdelen van het bedrijf. Deze *belangen* en *afhankelijkheden* moeten beschermd worden om ernstige bedrijfseconomische of maatschappelijke schade te voorkomen.

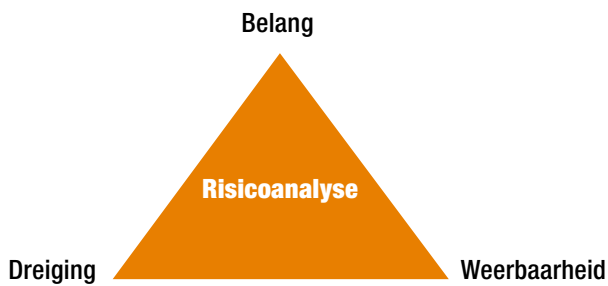
In de dreigingsanalyse worden kwaadwillende personen en hun activiteiten onderzocht. Hier staat de kans op de *dreiging* centraal. In dit geval: de terroristische dreiging.

In de kwetsbaarheidsanalyse gaat het om de *weerbaarheid* van een bedrijf. Als deze tekortschiet kan het bedrijf kwetsbaar zijn voor terroristische aanslagen.

In de risicoanalyse worden de cruciale belangen en afhankelijkheden, de kans op dreigingen en de weerbaarheid van een bedrijf aan elkaar gerelateerd. Dat levert een beeld op van de risico's van een bedrijf.

Om een goede risicoanalyse uit te voeren is kennis en informatie nodig over het bedrijf, over concrete en potentiële

dreigingen én over maatregelen die de weerbaarheid van een bedrijf verhogen. Doel van een risicoanalyse is om in te spelen op ernstige risico's van nu en in de nabije toekomst.



Verschillende organisaties, commerciële instellingen of adviesbureaus hanteren diverse methoden om risicoanalyses op te stellen. Ook zijn er risicoanalysemethoden die specifiek bedoeld zijn om beveiligingsmaatregelen te evalueren. In deze handreiking spreken we geen voorkeur uit voor één van deze methodieken. We geven slechts aan uit welke elementen een risicoanalyse hoort te bestaan.

Een risicoanalyse kan op verschillende manieren worden uitgevoerd. Het is mogelijk om een adviesbureau in te schakelen voor een gedegen analyse. Dit is aan te bevelen voor bedrijven die menen dat ze veel risico lopen of voor grotere bedrijven. Ook is het mogelijk met een aantal gelijksoortige bedrijven een gezamenlijke analyse uit te voeren. Hoe dan ook, het is belangrijk om in ieder geval een beproefde methodiek te hanteren en deskundigen te betrekken bij de verschillende onderdelen van de analyse. Voor kleinere bedrijven is het misschien niet mogelijk een analyse op te laten stellen door een extern bureau.

Het volgende schema kan (dan) helpen bij de uitvoering van een minder omvangrijke risicoanalyse. Het illustreert een cyclus voor risicomangement. Aan de hand van zes stappen kunnen de risico's van een bedrijf worden gerangschikt en benoemd. Dit vormt de basis voor (aanvullende) maatregelen om risico's te verminderen.



2. AFHANKELIJKHEIDSANALYSE

De afhankelijkheidsanalyse biedt zicht op de belangen van bedrijven. Denk aan mensen, bedrijfsprocessen, cruciale bedrijfselementen, grondstoffen, objecten of locaties. Het gaat om belangrijke waarden die kunnen worden aangetast en waarvan een bedrijf afhankelijk is.

Hieronder volgen een paar invalshoeken om de belangen en de afhankelijkheden van bedrijven te verhelderen:

- **mensen en hun veiligheid** zijn natuurlijk van het grootste belang voor iedere organisatie. Elk bedrijf moet de fysieke veiligheid van mensen kunnen waarborgen;
- **informatie** kan uniek, kostbaar, imagogevoelig, vertrouwelijk of cruciaal zijn voor de continuïteit of concurrentiepositie van een bedrijf. De beschikbaarheid, vertrouwelijkheid of de integriteit van de informatie moet dan ook worden veiliggesteld;
- **bedrijfsprocessen** zijn vaak cruciaal voor de continuïteit of concurrentiepositie van een bedrijf. Deze processen mogen niet of zo min mogelijk worden verstoord;
- **grondstoffen, productiemiddelen, producten en diensten** kunnen kostbaar en aantrekkelijk zijn voor kwaadwillenden. Het is dan ook belangrijk om de beschikbaarheid en integriteit hiervan te waarborgen.

Een goede afhankelijkheidsanalyse geeft inzicht in de belangen die het bedrijf onderkent en de omvang ervan. Ook geeft de analyse aan waarvan die belangen afhankelijk zijn. Zo kan bepaalde informatie cruciaal voor een bedrijf zijn. Om deze informatie te beschermen is het bedrijf afhankelijk van een betrouwbaar computersysteem. Mede op basis van de afhankelijkheidsanalyse krijgen bedrijven inzicht in de aard en omvang van de schade die een ernstig incident kan aanrichten. Dit noemen we ook wel het effect of de ernst van een incident. Deze schade kan van bedrijfseconomische of meer maatschappelijke aard zijn. Een categorisering en rangschikking van de ernst van mogelijke schades vormt de basis voor de risicoanalyse.

3. DREIGINGSANALYSE

Als de belangen en de afhankelijkheden van een bedrijf zijn benoemd en gerangschikt, moeten we systematisch bekijken hoe die belangen kunnen worden bedreigd. Wie kunnen een belang schaden en hoe gaan ze te werk?

Een dreigingsanalyse spreekt zich uit over (potentiële) dreigingen. Bij deze analyse is het verstandig eerst mogelijke kwaadwillende personen zoals terroristen in kaart te brengen. Wie heeft de kennis, kunde en intentie om specifieke bedrijven schade toe te brengen? Vervolgens moeten we vaststellen met welke middelen en met welke methoden terroristen te werk kunnen of zullen gaan.

Om een dreigingsanalyse op te stellen, kunnen bedrijven gebruikmaken van de informatie uit hoofdstuk 2, waarin de terroristische dreiging centraal staat. Aanvullende informatie staat op www.aivd.nl en www.nctb.nl

Om een inschatting te maken van dreiging die uitgaat van bijvoorbeeld criminelen, moeten bedrijven andere bronnen en deskundigen raadplegen.

Een categorisering en inschatting van de kans op een terroristische dreiging of een aanslag is de tweede bouwsteen voor de risicoanalyse.

4. KWETSBAARHEIDSANALYSE

De kwetsbaarheidsanalyse onderzoekt de kwetsbaarheid van bedrijven voor terroristische activiteiten. Het legt een relatie tussen de methoden en de middelen van terroristen en de weerbaarheid van het bedrijf daartegen. De methoden en middelen die terroristen kunnen of zullen gebruiken, vloeien voort uit de dreigingsanalyse. Welk bedrijf terroristen uitzoeken is afhankelijk van de aantrekkelijkheid van het bedrijf en de genomen beveiligingsmaatregelen. De weerbaarheid van een bedrijf kunnen we onderzoeken en eventueel verbeteren aan de hand van de vijf schakels van de veiligheidsketen: proactie, preventie, preparatie, respons en nazorg.

De veiligheidsketen bestaat uit vijf schakels:

Proactie: voorkomen of wegnemen van structurele oorzaken van onveiligheid;

Preventie: voorkomen van directe oorzaken van onveiligheid en beperken van de gevolgen van eventuele inbreuken op die veiligheid;

Preparatie: voorbereiden op het optreden bij een aanslag;

Respons: bestrijden en beperken van de nadelige gevolgen van een aanslag en hulp verlenen. Soms gebruiken we voor het woord respons ook 'repressie';

Nazorg: activiteiten gericht op het verhelpen van de gevolgen van een aanslag en de terugkeer naar de 'normale' situatie.

Hieronder beschrijven we de aard van de beveiligingsmaatregelen per schakel in de veiligheidsketen.

- **proactieve maatregelen** moeten voorkomen dat kwetsbaarheden ontstaan. Een bedrijf kan bijvoorbeeld bedrijfs-onderdelen naar een minder risicovolle locatie verplaatsen;
- **preventieve maatregelen** verkleinen de kwetsbaarheid en dus de kans op een incident. Voorbeelden hiervan zijn goed hang- en sluitwerk aanbrengen, een toegangscontrole instellen en virusscanners gebruiken;
- **preparatieve maatregelen** zijn gericht op een goede voorbereiding op incidenten. Een bedrijf kan bijvoorbeeld een ontruimingsplan opstellen voor het personeel en geregeld oefenen;
- **responsieve maatregelen** moeten de directe nadelige gevolgen van een incident beperken. Denk aan het inzetten van blusmiddelen, het organiseren van de eerste hulp en het managen van de crisis;
- **nazorgmaatregelen** moeten de bedrijfscontinuïteit en de teruggang naar de normale situatie bevorderen. Een voorbeeld is het regelen van een uitwijklocatie.

Type analyse	Focus op	Leidt tot
Afhankelijkheidsanalyse	aard en omvang van de bedrijfsbelangen	inschatting van de schade bij een incident
Dreigingsanalyse	<ul style="list-style-type: none"> • potentiële dreiging • terroristen • middelen en methoden 	inschatting van de kans op terroristische acties of incidenten
Kwetsbaarheidsanalyse	<ul style="list-style-type: none"> • weerbaarheid • maatregelen 	inschatting van de weerbaarheid van het bedrijf tegen terroristische activiteiten
Risicoanalyse	<ul style="list-style-type: none"> • belangen • potentiële dreiging • weerbaarheid 	inschatting van de ernst van de schade die incidenten ondanks de weerbaarheid van een bedrijf veroorzaken
Kosten- en batenanalyse	<ul style="list-style-type: none"> • effect / baten van de maatregelen • kosten van de maatregelen 	inschatting van de meest kosteneffectieve maatregelen: keuze van aanvullende maatregelen

5. RISICOANALYSE

De risicoanalyse brengt de belangen, dreigingen en weerbaarheid van het bedrijf bij elkaar. Het geeft inzicht in de risico's, welke risico's acceptabel zijn en tegen welke risico's het bedrijf maatregelen moeten nemen.

De risicoanalyse maakt de ernst en het effect van de meest waarschijnlijke terroristische acties duidelijk en houdt rekening met de weerbaarheid van het bedrijf.

De risicoanalyse betreft de resultaten uit de andere analyses:

- de kans op dreigingen en aanslagen;
- de weerbaarheid van het bedrijf tegen specifieke dreigingen of activiteiten;
- de ernst van de schade die incidenten ondanks de weerbaarheid van het bedrijf veroorzaken.

De kans op incidenten uit de dreigingsanalyse wordt concreter in het licht van de bestaande én ontbrekende weerbaarheid (maatregelen) uit de kwetsbaarheidsanalyse.

Sommige incidenten zullen bij nader inzien door de al aanwezige maatregelen minder aannemelijk blijken te zijn. Zo kan

een bedrijf beschikken over informatie die voor terroristen interessant is. Als blijkt dat een bedrijf adequate beveiligingsmaatregelen heeft genomen, is de kans dat deze informatie misbruikt wordt - en daarmee de kans op een incident - kleiner.

De kans dat een bedrijf te maken krijgt met een terroristische aanslag is doorgaans veel lager dan bijvoorbeeld de kans op diefstal. Daar staat tegenover dat de schade door een terroristische aanslag veel ernstiger kan zijn dan de schade die door criminaliteit wordt veroorzaakt.

In de risicoanalyse wordt de kans op een terroristische aanslag daarom gerelateerd aan de ernst van de schade die daaruit kan voortkomen. Dit noemen we ook wel effect. Het resultaat is een waardering van het risico. Een veel gebruikte formule hiervoor is:

Risico = Kans X Effect

Nadat de risico's in een rangorde geplaatst zijn, geeft het bedrijf aan welke risico's acceptabel zijn en tegen welke risico's het aanvullende maatregelen moet nemen.

Deze tabel laat zien hoe de afhankelijkheidsanalyse, dreigingsanalyse, kwetsbaarheidsanalyse en risicoanalyse met elkaar samenhangen.

6. KOSTEN- EN BATENANALYSE

De kosten- en batenanalyse bekijkt de aanvullende maatregelen die de geconstateerde risico's uit de risicoanalyse kunnen verminderen. Het is belangrijk om alle fasen uit de veiligheidsketen hierbij te betrekken en alle mogelijke maatregelen te inventariseren.

Aan de hand van deze maatregelen is het mogelijk de vermindering van risico's, ofwel de baten, van de maatregelen te bepalen. Centraal staat de vraag of de risico's echt minder worden door de maatregelen. Om het effect van deze maatregelen te beoordelen is enige deskundigheid vereist. Particuliere adviseurs kunnen deze expertise leveren. De volgende stap is het afzetten van de baten tegen de kosten

van de maatregelen. Daardoor wordt duidelijk welke maatregelen het meest kosteneffectief zijn. Staan de kosten in een acceptabele verhouding tot de baten? Aan de hand van een kosten- en batenoverzicht kan het bedrijf aanvullende maatregelen samenstellen. Het bedrijf is zelf verantwoordelijk voor deze afweging van kosten en baten en voor de keuze van de maatregelen. Met andere woorden: bedrijven bepalen zelf het risico dat ze willen lopen.

Na de keuze voor maatregelen is het mogelijk de kwetsbaarheidsanalyse en de risicoanalyse op onderdelen bij te stellen. De nieuwe uitkomst van de risicoanalyse geeft dan zicht op de beheersbaarheid en de acceptatie van de verschillende risico's door het bedrijf.

