# Handreiking Risicoanalyse

10 praktische modellen voor de risicoanalist

# Wat is het NAVI

In het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) werken overheid en bedrijfsleven samen aan de verbetering van de bescherming van de vitale infrastructuur in Nederland tegen moedwillig menselijk handelen. Deze bescherming heet security. In haar activiteiten richt het NAVI zich op fysieke, personele, organisatorische en digitale dreigingen.

Het NAVI ondersteunt beheerders en eigenaren van de vitale infrastructuur en de overheden op drie manieren:

### Veilig platform voor informatie-uitwisseling

Het NAVI geeft de gelegenheid om binnen een vertrouwde omgeving, met elkaar informatie uit te wisselen. Dit gebeurt zowel in een grotere openbare setting als in kleine besloten bijeenkomsten. Het NAVI brengt partijen bij elkaar, bijvoorbeeld via het organiseren en ondersteunen van kennis- en informatieknooppunten. Hierin komen partijen bij elkaar om informatie te delen en over beveiligingsonderwerpen te spreken.

### Aanbieden van kennis en expertise

Het NAVI biedt zelf kennis en expertise aan en stelt de betrokken partijen in staat om kennis en informatie binnen de vitale sectoren in Nederland te delen. Kennis en informatie worden op verschillende manieren beschikbaar gesteld, onder meer door het organiseren van bijeenkomsten, via de website en via een kennisbank.

### Nationaal en internationaal contactpunt

Het NAVI is een nationaal en internationaal contactpunt voor vragen en advies over security binnen de vitale infrastructuur en onderhoudt en ontwikkelt een breed netwerk. Tevens fungeert het NAVI als ontmoetingsplek voor de betrokken partijen binnen de vitale infrastructuur voor zowel overheidspartijen, kennisinstellingen in binnen- en buitenland, als bedrijven.

Voor meer informatie over het NAVI kunt u terecht op de website: www.navi-online.nl

# Inhoudsopgave

# 1. Voorwoord

Er zijn vele risicoanalysemethodieken beschikbaar op de markt. De scope van die risicoanalyses is erg divers. Zo zijn er bijvoorbeeld risicoanalyses voor bijvoorbeeld financiële, commerciële en strategische risico's, van informatiebeveiliging (CRAMM) en van gezondheid (ARBO-risico's en bedrijfsveiligheid).

Het doel van een risicoanalyse binnen de vitale infrastructuur is zicht te krijgen op risico's van deze infrastructuur voor de burgers en bedrijven in Nederland. Bij deze risicoanalyses worden zowel risico's onderzocht die samenhangen met de continuïteit van die infrastructuur en de leveringszekerheid van producten en diensten voor de maatschappij als ook risico's die direct veel slachtoffers veroorzaken of het milieu ernstig schaden (bijvoorbeeld door een explosie of een emissie van een gevaarlijke stof).

In deze handreiking wordt - op basis van de vele methodieken die er zijn - een generieke methodiek beschreven waarin (1) alle relevante stappen van een risicoanalyse aan de orde komen, (2) die zich specifiek richt op risico's aangaande moedwillige verstoring (security) en (3) die toe te passen is in alle vitale sectoren (dus niet sectorspecifiek is).

De handreiking is primair bedoeld voor functionarissen binnen de vitale infrastructuur die verantwoordelijk zijn voor risicomanagement en security. Deze handreiking geeft gebruikers handvatten om samen met anderen een risicoanalyse uit te voeren.

Deze handreiking is een revisie van de eerste Handreiking Risicoanalyse die het NAVI in 2008 heeft uitgebracht. In de nieuwe handreiking zijn de opgedane ervaringen in risicoanalyses meegenomen. Op veler verzoek is gekozen voor het bieden van meer concrete handvatten, namelijk door modellen, methoden, technieken en classificaties aan te reiken.

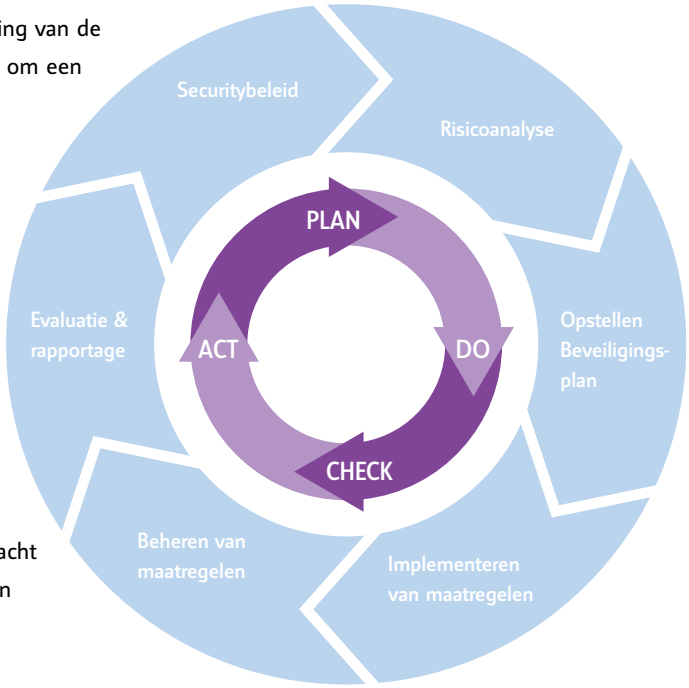
Indien u na het lezen van de handreiking vragen heeft, ondersteuning wenst bij het uitvoeren van (onderdelen van) uw risicoanalyse of uw ervaringen met het gebruik van deze handreiking wilt delen, dan kunt u contact opnemen met het NAVI. U kunt dat doen per mail via info@navi-online.nl of telefonisch via 070-376 59 50.

# 2. Inleiding

In een risicoanalyse wordt een inschatting gemaakt van de grootte van verschillende risico's die een organisatie kunnen bedreigen, onder meer door te bezien wat de waarschijnlijkheid en de mogelijke impact ervan zijn.

De risicoanalyse staat niet op zichzelf, maar is doorgaans onderdeel van de cyclus van het Security Management Systeem (SMS) van een organisatie. Het SMS bestaat uit een aantal volgtijdelijke stappen waarvan de risicoanalyse er één is.

Het SMS begint doorgaans met het vaststellen van het securitybeleid. Daarna volgt de stap van de risicoanalyse, waarvoor deze handreiking modellen en checklists biedt. Vervolgens kan op basis van de gevonden risico's een beveiligingsplan worden opgesteld om de weerstand tegen de risico's te verhogen. Op basis van dat plan kunnen maatregelen worden geïmplementeerd, beheerd en geëvalueerd. De evaluatie kan aanleiding zijn het securitybeleid te herijken (en opnieuw een risicoanalyse uit te voeren). Op die wijze vinden deze stappen iteratief en periodiek plaats. Hierna volgt een schematische weergave van de positie van de risicoanalyse in een SMS.




Een risicoanalyse beoogt een bijdrage te leveren aan de borging van de business continuity. Er kunnen verschillende aanleidingen zijn om een risicoanalyse uit te voeren:

- **Ontwikkelingen in de activiteiten van de organisatie.**
  Nieuwe of andere activiteiten kunnen aanleiding geven nieuwe risico's nader te onderzoeken.

- **Ontwikkelingen in het dreigingsniveau.**
  Het dreigingsniveau is aan verandering onderhevig, bijvoorbeeld wanneer een moedwillige verstoring heeft plaatsgevonden bij een soortgelijke organisatie (in Nederland of het buitenland), er een reorganisatie plaatsvindt die kan leiden tot ontevreden werknemers of de organisatie in de publiciteit staat en daarmee de aandacht trekt van potentiële daders. Ook kan er sprake zijn van een verhoogd alerteringsniveau.

- **Ontwikkelingen in de omgeving.**
  Ook omgevingsontwikkelingen kunnen aanleiding vormen voor het opnieuw uitvoeren van een risicoanalyse. Bijvoorbeeld wanneer een woonwijk wordt gerealiseerd in de nabijheid van de BRZO-locatie (Besluit Risico's Zware Ongevallen-locatie) - een eventuele emissie kan dan een groter effect hebben - of wanneer zich nieuwe buurbedrijven vestigen met een ander beveiligingsbeleid dan hun voorgangers (met mogelijke effecten op de beveiliging van de eigen organisatie).

- **Planning & control-cyclus van de organisatie.**
  De risicoanalyse vormt input voor het beveiligingsplan en kan ertoe leiden dat de organisatie maatregelen wil implementeren die investeringen vergen. In dat geval is het van belang aan te sluiten bij de planning van de begrotingscyclus, omdat deze investeringen dan kunnen worden afgewogen tegen andere investeringen die de organisatie mogelijk wil plegen.

# 3. Vijf stappen van de risicoanalyse

Een risicoanalyse bestaat uit vijf opeenvolgende stappen. Hierna worden de stappen kort beschreven.

1. **Voorbereidingsfase.** In de voorbereidingsfase stelt de risicoanalist de afbakening voor de risicoanalyse vast en maakt een plan van aanpak waarin de betrokkenheid van de eigen organisatie en de externe experts en adviseurs wordt geborgd.
   Na de voorbereidingsfase is het plan van aanpak uitgewerkt, is de betrokkenheid van de mensen die hun kennis en expertise beschikbaar stellen geregeld en is helder waarop de risicoanalyse wel en niet betrekking heeft (de afbakening).

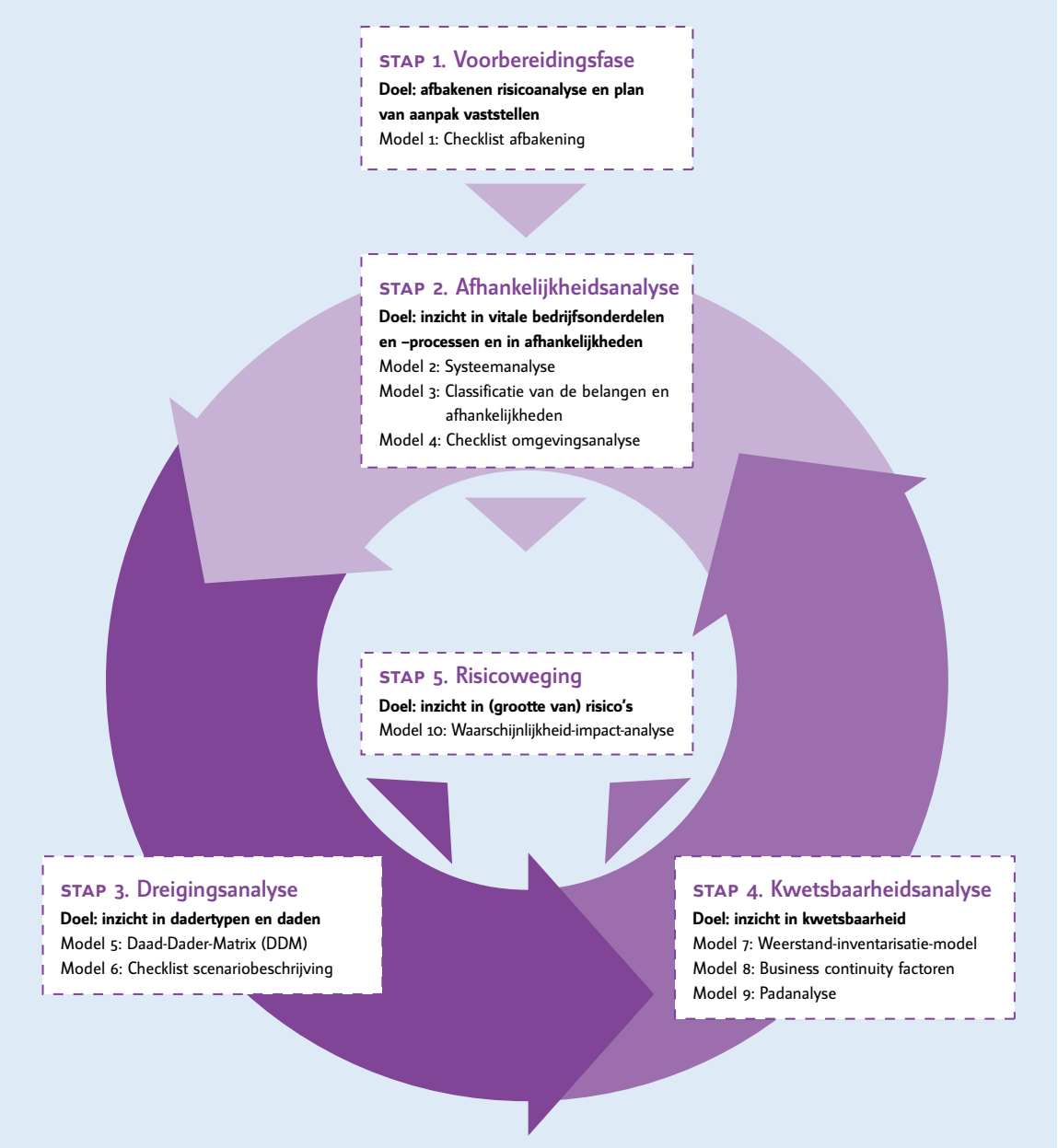
2. **Afhankelijkheidsanalyse.** Bij deze analyse wordt in kaart gebracht hoe de organisatie functioneert, welke interne en externe factoren daarbij een rol spelen en welke belangen in de risicoanalyse centraal zullen staan. De belangen van een organisatie, die wellicht bescherming verdienen kunnen in verschillende categorieën worden ingedeeld zoals: mensen, informatie, producten, diensten, bedrijfsprocessen en bedrijfsmiddelen. Daarnaast wordt in kaart gebracht van welke externe factoren deze belangen afhankelijk zijn: zoals energie, grondstoffen, koelwater, telecom en transport. Na de afhankelijkheidsanalyse heeft de risicoanalist zicht op de verschillende belangen en afhankelijkheden van de organisatie.

3. **Dreigingsanalyse.** Hierin worden de typen opponenten (kwaadwillende personen) en hun ongewenste activiteiten geanalyseerd. In deze handreiking wordt daarbij gebruik gemaakt van een Daad-Dader-Matrix waarin combinaties van dadertypen en daden worden onderscheiden die systematisch worden onderzocht. Mogelijke dadertypen zijn bijvoorbeeld terroristen, hackers en gefrustreerde (ex-)medewerkers. Mogelijke daden zijn bijvoorbeeld sabotage, diefstal, ICT uitschakelen of een bompakket plaatsen. In het kader van de bescherming van de vitale infrastructuur zijn vooral dreigingen relevant die op enige wijze de continuïteit en leveringszekerheid ernstig aantasten, dan wel de bevolking of het milieu ernstige schade kunnen toebrengen.
   Na de dreigingsanalyse heeft de risicoanalist zicht op de meest relevante dreigingen (daad-dader-combinaties).

4. **Kwetsbaarheidsanalyse.** In de kwetsbaarheidanalyse wordt het weerstandsvermogen van de organisatie in kaart gebracht, uitgaande van de mogelijke dreigingen, die in de dreigingsanalyse naar voren zijn gekomen (en uitgaande van de bescherming van de bedrijfsmiddelen en –processen en de afhankelijkheden, die in de afhankelijkheidsanalyse naar voren zijn gekomen). Bij weerstand kan worden gedacht aan de maatregelen die zijn genomen, bijvoorbeeld fysieke weerstandsmaatregelen (waaronder hekken en compartimentering), digitale weerstandsmaatregelen, organisatorische weerstandsmaatregelen en personele weerstandsmaatregelen.
   Na de kwetsbaarheidsanalyse heeft de risicoanalist zicht op de weerstand van de organisatie tegen mogelijke dreigingen en de kwetsbaarheid van de organistaie (in het geval van een gebrek aan weerstand op bepaalde onderdelen).

5. **Risicoweging.** De risicoweging is de laatste stap in de risicoanalyse. De drie voorgaande analyses (die van de afhankelijkheden, dreigingen en weerstand) vormen de input hiervoor. De gevonden dreigingen die de bedrijfsmiddelen en -processen en de afhankelijkheden bedreigen en waartegen tot op heden relatief weinig weerstand bestaat, worden geschat op hun waarschijnlijkheid en op de mogelijke impact (waaronder economische schade, slachtoffers en gewonden). Risico is vervolgens waarschijnlijkheid x impact. Daardoor ontstaat een indeling van de gevonden risico's: risico's waarvan de waarschijnlijkheid relatief klein is versus risico's waarvan de waarschijnlijkheid relatief groot is. Tevens is er inzicht op risico's met relatief veel potentiële impact versus risico's met relatief weinig potentiële impact.
   Na de risicoweging heeft de risicoanalist zicht op de risico's en op de relatieve grootte ervan. Dat vormt de basis voor een discussie die ná de risicoanalyse kan worden gevoerd, namelijk de discussie of de gevonden risico's aanleiding vormen om aanvullende maatregelen te nemen.

In de hoofdstukken hierna wordt per stap een uitgebreide toelichting gegeven waarbij tevens modellen en checklists worden beschreven die bij deze stappen door de risicoanalist kunnen worden gehanteerd. In het schema hierna wordt in een overzicht weergegeven welke modellen en checklists dat zijn.




Via het doorlopen van de vijf stappen en het toepassen van de modellen, wordt stapsgewijs inzicht verkregen in cruciale bedrijfsmiddelen en -processen (die niet mogen uitvallen), in de daad-dader-combinaties (die een bedreiging vormen voor die cruciale bedrijfsonderdelen) en in de kwetsbaarheid van de organisatie als het gaat om de bescherming tegen de ongewenste daden. Op basis daarvan kunnen waarschijnlijkheid en de impact worden geschat en daarmee de grootte van het risico. In de risicotabel hierna wordt duidelijk dat deze verschillende onderdelen van de analyse informatie opleveren die uiteindelijk leidt tot het kunnen inschatten van de risico's.

De tabel hierna kan worden gebruikt als een soort van overzichtstabel die telkens na het doorlopen van een stap in de risicoanalyse kan worden ingevuld. Na de afhankelijkheidsanalyse kunnen de eerste twee kolommen worden ingevuld. In de eerste kolom kunnen de bedrijfsmiddelen en -processen worden ingevuld die in de tweede kolom

| Afhankelijksheidsanalyse | | Dreigingsanalyse | | Kwetsbaarheidsanalyse | | Risicoweging | | |
|---|---|---|---|---|---|---|---|---|
| Belangen en afhankelijkheden | Classificatie | Relevante daad-dader-combinaties | Classificatie | Kwetsbaarheden | Classificatie | Waarschijn-lijkheid (p) | Impact (e) | Risico (p x e) |
| | | | | | | | | |
| | | | | | | | | |

van een classificatie kunnen worden voorzien. Die classificatie geeft uitdrukking aan een prioritering. Immers, niet elk bedrijfsproces en niet elk bedrijfsmiddel is even belangrijk, waardoor het van belang is om onderscheid te maken. Na de dreigingsanalyse kunnen de derde en vierde kolom worden ingevuld. De daad-dader-combinaties die een bedreiging vormen voor de bedrijfsmiddelen en -processen in de eerste kolom, worden ingevuld in derde kolom. In de vierde kolom worden de daad-dader-combinaties geclassificeerd, zodat ook op dat onderdeel een prioritering ontstaat. Na de kwetsbaarheidsanalyse kunnen de vijfde en zesde kolom worden ingevuld. Op die wijze wordt in kaart gebracht hoe kwetsbaar de bedrijfsmiddelen en –processen zijn in het licht van de mogelijke dreigingen.

Tot slot wordt in de stap van de risicoweging kolom zeven tot en met negen ingevuld: de waarschijnlijkheid op die daad-dader-combinatie, de impact en het restrisico. Op die wijze ontstaat een compleet overzicht na afloop van de risicoanalyse.

# 4. Stap 1: Voorbereidingsfase

## Kern van de voorbereidingsfase

In de voorbereidingsfase maakt de risicoanalist een plan van aanpak. Onderwerpen die in het plan van aanpak aan de orde kunnen komen zijn: fasering, doorlooptijd, planning, oplevering van eventuele tussenrapportages en omgang met de vertrouwelijkheid van de risicoanalyse. Het NAVI heeft overigens voor de omgang met vertrouwelijke informatie een classificatiemethode opgesteld die beschikbaar is op www.navi-online.nl.

In de aanpak is het voorts van groot belang om de betrokkenheid van de eigen organisatie en van externen (die bijvoorbeeld specifieke competenties en expertise inbrengen) goed te waarborgen. De interne betrokkenheid betreft twee dimensies.

- Ten eerste is het van belang het verantwoordelijk management (bijvoorbeeld directie, Raad van Bestuur, MT) te betrekken en te engageren bij de risicoanalyse. Zij dienen opdracht te geven voor het uitvoeren van de risicoanalyse en te beslissen bij belangrijke tussenstappen en besluitvormingsmomenten. Immers, zij hebben doorgaans ook een belangrijke rol bij het beslissen over de follow up naar aanleiding van de risicoanalyse.

- Ten tweede is het van belang de binnen de organisatie aanwezige kennis zo goed mogelijk aan te wenden, bijvoorbeeld door de eigen medewerkers te vragen naar de in hun ogen kwetsbare plekken in de beveiliging. Hun betrokkenheid in deze fase van de risicoanalyse kan bovendien een positief effect hebben op het draagvlak van en de medewerking aan mogelijke maatregelen, die in een later stadium genomen worden om de gevonden risico's te beperken.

Bij de externe betrokkenheid kan worden gedacht aan het betrekken van organisaties of personen met specifieke expertise die kunnen bijdragen aan de kwaliteit van de risicoanalyse. Voorbeelden van externen zijn: particuliere beveiligingsorganisaties, organisatie-adviesbureau's, brancheorganisaties, politie, gemeente, het vakdepartement, het NAVI, Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Nationaal Coördinator Terrorismebestrijding (NCTb). Er is een aantal gebieden van expertise te onderscheiden die relevant zijn bij het maken van een goede risicoanalyse voor de vitale infrastructuur.

- Kennis over en ervaring met het uitvoeren van risicoanalyses.

- Expertise op het gebied van security en security-management. Er zijn diverse adviesbureau's die expertise hebben op het terrein van moedwillig menselijk handelen en de maatregelen die daartegen kunnen worden genomen.

- Kennis over de reële fysieke en digitale dreigingen. Op dat punt kunnen bijvoorbeeld regionale politiekorpsen, Regionale Inlichtingen Diensten (RID) en het NAVI kennis en expertise inbrengen die helpt om een beeld te vormen van de meest reële dreigingen (en de minder relevante dreigingen). Brancheverenigingen kunnen in dat licht vaak ook veel betekenen, bijvoorbeeld omdat ze goed op de hoogte zijn van incidenten die hebben plaatsgevonden in de sector.

- Expertise van de verschillende security domeinen zoals: ICT-beveiliging, fysieke beveiliging, personele beveiliging, persoonsbeveiliging en security awareness.

- Kennis en ervaring van concullega's die al eerder ervaringen hebben opgedaan met een soortgelijke risicoanalyse.

Tot slot is het van belang om een eenduidige afbakening te maken. De checklist hierna kan daarbij behulpzaam zijn.

## Model 1: Checklist afbakening

Het is van belang de risicoanalyse goed af te bakenen op basis van de zes aspecten hierna:

- **Onderwerp** van de risicoanalyse. Gaat het om een specifiek bedrijfsonderdeel/bedrijfsproces op een specifieke vestigingslocatie, gaat het om een hele locatie of gaat het om alle locaties in Nederland (of wereldwijd)?

- **Scope** van de risicoanalyse. Gaat het om risico's rondom moedwillige verstoring (security) of gaat het om een heel brede all hazards-risicoanalyse waarin alle risico's worden meegenomen, bijvoorbeeld ook natuurrampen en het falen van machines en mensen zonder dat er opzet in het spel is (zoals graafwerkzaamheden waardoor een voor de organisatie belangrijke kabel of leiding wordt beschadigd). Als het alleen over moedwillige verstoring gaat: is het dan over de volle breedte van moedwillige verstoring of een specifiek onderdeel daarvan? Bijvoorbeeld alleen het binnendringen door externen (dieven, activisten, terroristen), alleen de mogelijke daden van (gefrustreerde) medewerkers of bijvoorbeeld alleen de ICT-georiënteerde risico's?

- **Typen effecten en schade** die worden meegenomen. Gaat het alleen om schade voor de organisatie of ook om schade die buiten de poort ontstaat, bijvoorbeeld in de omgeving (als gevolg van milieuschade of een emissie van een gevaarlijke stof) of bij klanten van de organisatie (omdat de eigen organisatie geen producten meer kan aanleveren en eventueel afspraken met afnemers niet kan nakomen omdat het proces is verstoord)? Gaat het alleen om economische schade of ook om 'doden buiten de poort' (of juist over allebei)?

- **Diepgang** van de analyse. Wordt de risicoanalyse uitgevoerd op hoofdlijnen (die dient als een eerste quick scan op basis waarvan nader onderzoek kan worden gedaan naar de risico's) of wordt juist heel erg de diepte in gegaan voor details (omdat de hoofdlijnen al bekend zijn en het er nu om gaat om investeringsvoorstellen te bezien op hun veiligheidswinst en hun kosten en baten)?

- **Periode** waarop de risicoanalyse betrekking heeft. Enerzijds gaat het dan om de frequentie van de risicoanalyse: de periode tussen de huidige risicoanalyse en de volgende. Anderzijds gaat het om de risicohorizon: hoe ver wordt vooruitgekeken als het gaat om de risico's (alleen de risico's van nu of ook de risico's die zich als gevolg van een bepaalde ontwikkeling pas over vijf jaar aandienen)?

- **Mate waarin verplichtingen vanuit relevante wet- en regelgeving (compliance) direct kunnen worden meegenomen** in de analyse. Zo kan de risicoanalist bijvoorbeeld de risicoanalyse opvoeren als onderdeel van de te implementeren wet- en regelgeving. Te denken valt aan bijvoorbeeld de International Ship and Port facility Security code (ISPS-code), de Authorised Economic Operator (AEO) of het Besluit Risico's Zware Ongevallen-wetgeving (BRZO-wetgeving). Daarnaast kan de risicoanalist in de stap van de kwetsbaarheidanalyse de maatregelen in ogenschouw nemen die wettelijk nog moeten worden geïmplementeerd.

In bijlage 1 is een checklist opgenomen die puntsgewijs de onderdelen van de voorbereiding weergeeft.

## Resultaat

Na de voorbereidingsfase heeft de risicoanalist de afbakening voor de risicoanalyse vastgesteld. Daarnaast is een plan van aanpak gemaakt en vastgesteld waarin onder meer de betrokkenheid van de eigen organisatie ('interne' betrokkenheid) en de 'externe' betrokkenheid van experts en adviseurs is vormgegeven.

# 5. Stap 2: Afhankelijkheidsanalyse

## Kern van de afhankelijkheidsanalyse

In de afhankelijkheidsanalyse wordt in kaart gebracht - gegeven de gekozen afbakening van de risicoanalyse in de vorige stap - hoe de organisatie functioneert, welke interne en externe factoren daarbij een rol spelen en welke belangen in de risicoanalyse centraal zullen staan. De belangen van een organisatie die wellicht bescherming verdienen kunnen in verschillende categorieën worden ingedeeld zoals: mensen, informatie, producten, diensten, bedrijfsprocessen en bedrijfsmiddelen. Gezocht wordt naar die elementen van de organisatie die bij emissie, uitval, manipulatie of iets dergelijks de organisatie of de omgeving van de organisatie (grote) schade berokkenen. Daarbij kan het gaan om verschillende soorten schade: economische schade (geld, uren uitval), schade aan personen (doden of gewonden), schade aan het milieu (bijvoorbeeld door het lekken van een buisleiding) en schade aan imago.

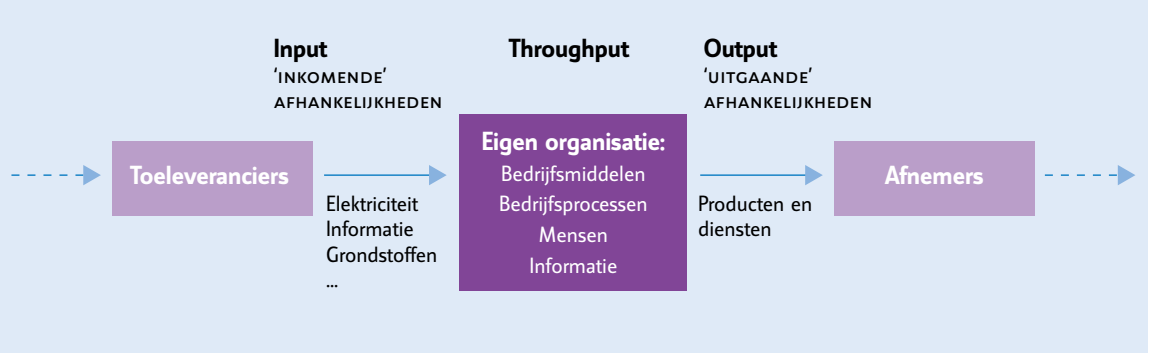
Daarnaast wordt in kaart gebracht van welke externe factoren deze belangen afhankelijk zijn, zoals energie, grondstoffen, koelwater, telecom en transport. Het betreft hier de zogenaamde afhankelijkheden.
Het is ook voorstelbaar dat bepaalde diensten of producten van de eigen organisatie een afhankelijkheid zijn voor een andere vitale organisatie. Deze intersectorale afhankelijkheden kunnen in de scope worden meegenomen.

De risicoanalist kan zichzelf de volgende vraag stellen om de belangen en afhankelijkheden te identificeren: Wat zijn de cruciale (en gevaarlijke) bedrijfsonderdelen en -processen die in geen enkel geval mogen worden verstoord? Welke toevoer mag absoluut niet stagneren? Ook kunnen vragen worden gesteld vanuit de te voorkomen effecten: Wanneer is er sprake van zeer grote economische schade (of andere schade zoals politiek-maatschappelijke schade, milieuschade, gezondheidsschade en doden en gewonden buiten de poort)? Bij het beantwoorden van die vragen komen de verschillende belangen en afhankelijkheden naar voren.

Hierna worden drie modellen beschreven die behulpzaam kunnen zijn bij de afhankelijkheidsanalyse. Ten eerste de systeemanalyse waarbij de vitale processen en bedrijfsonderdelen in kaart worden gebracht, evenals de factoren waarvan die processen en onderdelen afhankelijk zijn. Ten tweede wordt een classificatiemodel beschreven waarmee de bedrijfsmiddelen en -processen kunnen worden gecategoriseerd in vier typen. Tot slot wordt een checklist beschreven ten behoeve van de uitvoering van een omgevingsanalyse.

## Model 2: Systeemanalyse

Een systeemanalyse kan behulpzaam zijn bij het genereren van inzicht in de belangen en afhankelijkheden. Hierna is een grafisch voorbeeld van een systeemanalyse weergegeven.




Een systeemanalyse is een model dat de gebruiker helpt om in kaart te brengen wat de belangrijke onderdelen en aspecten van de organisatie zijn en aan te geven wat er de organisatie 'in' gaat en wat er 'uit' komt. Kortom: alle stromen en externe toevoeren die een organisatie binnenkomen en die noodzakelijk zijn om te kunnen blijven functioneren (de afhankelijkheden) en de producten die er uiteindelijk 'aan de achterkant' uitkomen. In bijlage 2 bij deze handreiking is een lijst opgenomen die behulpzaam kan zijn bij deze systeemanalyse.
In aanvulling op deze systeemanalyse - die de bedrijfsprocessen centraal stelt - kan de risicoanalist nog een

verdiepingsslag maken door een schematische plattegrond te maken. Via die visualisatie wordt dan niet alleen duidelijk wat de vitale bedrijfsmiddelen en productieprocessen zijn, maar ook waar ze zich op het terrein bevinden. Dit inzicht kan van belang zijn om bijvoorbeeld ook de weerstand in kaart te kunnen brengen bij de kwetsbaarheidsanalyse. In bijlage 3 is een voorbeeld gegeven van zo'n schematische plattegrond.

Daarnaast kan tevens een organogram worden gemaakt. Daarmee wordt de inrichting van de organisatie inzichtelijk evenals wie de sleutelfunctionarissen in de organisatie zijn.

## Model 3: Classificatie van de belangen en afhankelijkheden

Middels de systeemanalyse zijn de bedrijfsprocessen en interne en externe afhankelijkheden schematisch in kaart gebracht. Daarna is het mogelijk deze onderdelen van het bedrijfsproces te beoordelen naar belangrijkheid voor de organisatie, bijvoorbeeld door ze te classificeren in vier klassen: A tot en met D. Een voorbeeld van een dergelijke classificatie voor bedrijfsprocessen is hierna opgenomen.

**Classificatie van de belangen en afhankelijkheden**

| Waardering | Classificatie | Beschrijving |
|---|---|---|
| Maatschappelijk vitaal | A=4 | **Nationaal belang**<br>Bij uitval of (grootschalige) verstoring van het bedrijfsproces vallen doden of gewonden (of worden mensen chronisch ziek) of ontstaat maatschappelijke ontwrichting (verstoring van het dagelijks leven), gebrek aan primaire levensbehoeften, ernstige economische schade, schade aan flora en fauna, (zeer) ernstige schade voor de Staat of haar bondgenoten of aantasting van de democratie, het Nederlands territorium of de internationale positie van Nederland. |
| Bedrijfsvitaal | B=3 | **Bestaansrecht (strategisch)**<br>In relatie tot de doelstellingen van de organisatie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop de organisatie direct wordt aangesproken; én/óf de organisatie krijgt 80% of meer van de inkomsten uit dit proces of het budget van de organisatie wordt voor meer dan 80% uitgeput door dit proces; én/óf als de activiteit uitvalt of niet goed verloopt, heeft dit ernstige consequenties voor het voortbestaan van de organisatie, brengt het de organisatie in grote problemen. Ook wel primaire processen genoemd. |
| Bedrijfskritisch | C=2 | **Noodzakelijke voorwaarde (bedrijfskritisch)**<br>Het bedrijfsproces kan als kritisch worden getypeerd als het een directe relatie heeft met het tot stand brengen van de noodzakelijke voorwaarden om producten/diensten te kunnen voortbrengen of als het rechtstreeks voortvloeit uit de doelstellingen van een organisatie; én/óf kan een ontwikkelpotentieel aan het proces worden toegekend en kan het dus in de toekomst belangrijker worden in verband met mogelijke veranderingen in de strategische doelstellingen van de organisatie; én/óf een aanzienlijk deel van de omzet wordt gegenereerd met dit proces of een aanzienlijk deel van het te besteden budget komt ten goede aan dit proces. Ook wel secundaire processen genoemd. |
| Ondersteunend | D=1 | **Indirecte relatie**<br>Er is sprake van een indirecte relatie met de hoofdactiviteiten van de organisatie; én/óf het ontbreken van het bijdragende proces heeft binnen het primaire proces slechts effectiviteits- en efficiëntieverliezen tot gevolg. Ook wel tertiaire processen genoemd. |

Organisaties kunnen ook een eigen classificatie hanteren die uitgaat van andere klassen die mogelijk beter passen bij de specifieke kenmerken van de organisatie. In ieder geval is het van belang dat er in deze stap van de analyse onderscheid wordt aangebracht tussen de zeer vitale en de minder vitale processen en bedrijfsmiddelen.

## Model 4: Checklist omgevingsanalyse

Ook de fysieke omgeving van de organisatie moet in kaart worden gebracht: het gebied buiten de poort. Daar zijn twee redenen voor. Ten eerste beïnvloedt die omgeving de aantrekkingskracht van de organisatie als doelwit van bepaalde dadertypen. Dit is bijvoorbeeld het geval indien er een woonwijk is gelegen in de omgeving van de organisatie die zeer gevaarlijke stoffen opslaat. Een emissie zou in dat geval tot relatief veel slachtoffers kunnen leiden. Zonder die woonwijk zou de organisatie een relatief minder aantrekkelijk doelwit kunnen zijn. Ten tweede is die omgeving van invloed op de mate waarin bepaalde ongewenste daden kunnen worden uitgevoerd. Zijn er vanuit de omgeving (van buiten het bedrijfsterrein) bijvoorbeeld ongehinderde zichtlijnen naar de opslagtanks met gevaarlijke stoffen? Is het mogelijk om ongemerkt verkenningsacties uit te voeren, bijvoorbeeld via aangrenzend braakliggend terrein of via buurbedrijven of via een flat aan de overkant van de weg?

Dus behalve een systeemanalyse en een schematische plattegrond van het bedrijfsterrein (zie bijlage 3) dient ook een omgevingsanalyse te worden gemaakt. Daarbij verdienen de volgende aspecten aandacht:

1. **Woningen.** Zijn er woningen in de nabije omgeving? Veel of weinig bewoners? Laagbouw of hoogbouw? Et cetera.
2. **Voorzieningen waar veel mensen komen.** Zijn er bijvoorbeeld stadions, pretparken, scholen en sport-accommodaties in de nabije omgeving? Of zijn er wel eens festiviteiten in de omgeving die heel veel mensen trekken (bijvoorbeeld een groot jaarlijks popfestival)? Et cetera.
3. **Bedrijfsterrein en buurbedrijven.** Is het een monosite (een terrein alleen voor de eigen organisatie) of is het een bedrijvenpark? Zijn de aanliggende bedrijfsterreinen en buurbedrijven wel of niet beveiligd? Et cetera.
4. **Braakliggend terrein en natuur.** Is er sprake van braakliggend terrein in de nabije omgeving? Is dat open of juist bebost? Is dat toegankelijk? Et cetera.
5. **Parkeerplaats.** Zijn er openbaar toegankelijke parkeerplaatsen buiten de bedrijfspoort (van waaruit mensen ongestoord kunnen observeren)? Is die parkeervoorziening bewaakt of niet bewaakt? Et cetera.
6. **Ontsluitingswegen.** Zijn er één of meer ontsluitingswegen vanaf het eigen bedrijfsterrein? Voor welke modaliteiten: voet, fiets, auto? Zijn die bewaakt of onbewaakt? Et cetera.
7. **Spoorlijnen.** Komt de spoorlijn en de trein tot binnen het bedrijfsterrein? Is het laadpunt binnen of buiten de poort? Is de toegangspoort bewaakt? Is er sprake van een doorgaande spoorverbindingen waarover ook treinen voor andere organisaties rijden (multigebruik)? Et cetera.
8. **Lucht.** Wat voor voorzieningen lopen boven het bedrijfsterrein langs? Hoogspanningslijnen? Vliegroutes? Bruggen en viaducten? Et cetera.
9. **Water.** Maakt de organisatie gebruik van toevoer via het water (haven, rivier)? Is de haven afgesloten? Is de aanlegplaats voor schepen afgesloten? Kunnen vissersboten, recreatief verkeer en andere schepen ongestoord in de buurt komen? Et cetera.

## Resultaat

Na de afhankelijkheidsanalyse heeft de risicoanalist zicht op de belangrijkste bedrijfsmiddelen en -processen, mensen (sleutelfunctionarissen), informatie en afhankelijkheden van de organisatie. Deze zijn bovendien geclassificeerd waardoor een prioritering is ontstaan. Bovendien heeft de risicoanalist zicht gekregen op de (fysieke) omgeving van de organisatie.

# 6. Stap 3: Dreigingsanalyse

## Kern van de dreigingsanalyse

Bij de dreigingsanalyse worden de typen opponenten (kwaadwillende personen) en de ongewenste activiteiten die zij moedwillig kunnen uitvoeren geanalyseerd.

Een belangrijk hulpmiddel daarbij is de Daad-Dader-Matrix (DDM). Daarbij wordt gebruik gemaakt van een groslijst aan dadertypen en een groslijst aan daden. Mogelijke dadertypen zijn bijvoorbeeld terroristen, hackers en gefrustreerde medewerkers. Mogelijke daden zijn bijvoorbeeld inbraak, diefstal, sabotage of een bompakket plaatsen. Na het uitvoeren van de DDM-analyse ontstaat een lijst met de meest relevante daad-dader-combinaties.

Met behulp van de checklist scenariobeschrijving kunnen de relevante daad-dader-combinaties worden uitgewerkt tot scenario's.

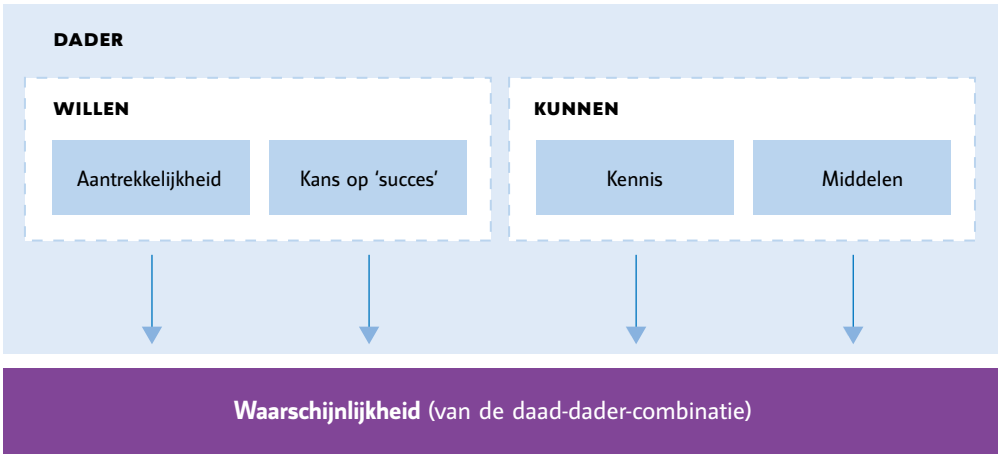
## Model 5: Daad-Dader-Matrix (DDM)

De Daad-Dader-Matrix is tot stand gekomen op basis van de ervaring van zowel inlichtingendiensten als het NAVI en is toegespitst op daden en daders die een dreiging kunnen vormen voor de continuïteit van vitale infrastructuur of de mogelijke effecten buiten de poort die uit deze daden kunnen voortkomen. In totaal gaat het om 14 typen daders en om 52 daden, die theoretisch gezien leiden tot 728 mogelijke combinaties. De term 'theoretisch' wordt hier gebruikt omdat niet alle combinaties logisch zijn. De lijst is niet-limitatief en zal voor elke organisatie verschillend kunnen worden aangevuld met daders en daden die voor die specifieke organisatie relevant kunnen zijn.

Door het toepassen van de Daad-Dader-Matrix kan de risicoanalist systematisch onderzoek doen naar mogelijke scenario's, gegeven de kenmerken van zijn eigen organisatie (bedrijfsterrein, personeelsbestand, vitale onderdelen, et cetera). Via het systematisch bestuderen van alle opties kan worden toegewerkt naar de meest relevante daad-dader-combinaties die in de volgende stappen van de risicoanalyse centraal zullen staan (bijvoorbeeld bij de padanalyse). Zo kan de risicoanalist ervoor kiezen om bijvoorbeeld een top 10 of top 20 daad-dader-combinaties te maken. In het overzicht hierna worden de 14 dadertypen en 52 typen daden weergegeven.

Een verklarende woordenlijst met betrekking tot enkele dadertypen en daden is opgenomen in bijlage 4.

De dreiging van een aanval is afhankelijk van een aantal factoren. Enerzijds van de motivatie van een dader om dat doel aan te vallen. Die motivatie wordt bepaald door de aantrekkelijkheid van het doel en de kans op een succesvolle aanval. Deze factoren geven samen een beeld van het 'willen' door de dader. Anderzijds wordt de dreiging op een aanval bepaald door de bij de dader beschikbare kennis en middelen om de actie daadwerkelijk uit te voeren. Deze factoren geven samen een beeld van het 'kunnen' door de dader. Het model hierna visualiseert dat.



| | Dadertypen | Verwarde persoon | Vandaal | Activist | Gewelddadige activist | Hacktivist | Scriptkiddie | Hacker | Gefrustreerde medewerker | Ontslagen medewerker | Lichte crimineel | Zware crimineel | Terrorist | Oneerlijke concurrent | Vijandige inlichtingendienst |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Daden** | | | | | | | | | | | | | | |
| **1.** | **Diefstal** | | | | | | | | | | | | | | |
| 1.1 | Insluiping/insluiting | | | | | | | | | | | | | | |
| 1.2 | Diefstal (goederen, informatie, et cetera) | | | | | | | | | | | | | | |
| 1.3 | Gelegenheidsdiefstal | | | | | | | | | | | | | | |
| 1.4 | Inbraak | | | | | | | | | | | | | | |
| 1.5 | (Roof)overval | | | | | | | | | | | | | | |
| 1.6 | Ramkraak | | | | | | | | | | | | | | |
| 1.7 | Heling | | | | | | | | | | | | | | |
| **2.** | **Fraude** | | | | | | | | | | | | | | |
| 2.1 | Bedrijfsfraude | | | | | | | | | | | | | | |
| 2.2 | Omkoping en corruptie | | | | | | | | | | | | | | |
| 2.3 | Witwassen | | | | | | | | | | | | | | |
| 2.4 | Afpersing en chantage | | | | | | | | | | | | | | |
| **3.** | **Spionage** | | | | | | | | | | | | | | |
| 3.1 | Afluisteren | | | | | | | | | | | | | | |
| 3.2 | Infiltratie | | | | | | | | | | | | | | |
| 3.3 | Bedrijfsspionage | | | | | | | | | | | | | | |
| **4.** | **Cyberaanval** | | | | | | | | | | | | | | |
| 4.1 | Hacking | | | | | | | | | | | | | | |
| 4.2 | Procesbesturingssystemen aanvallen (SCADA/EMS) | | | | | | | | | | | | | | |
| 4.3 | Wardriving | | | | | | | | | | | | | | |
| 4.4 | Wardialling | | | | | | | | | | | | | | |
| 4.5 | Website defacing | | | | | | | | | | | | | | |
| 4.6 | Sabotage van ICT (computervirus/(D)DoS) | | | | | | | | | | | | | | |
| **5.** | **Geweld** | | | | | | | | | | | | | | |
| 5.1 | Bedreiging en intimidatie | | | | | | | | | | | | | | |
| 5.2 | Ernstige (fysieke) bedreiging | | | | | | | | | | | | | | |
| 5.3 | Gijzeling, ontvoering en kaping | | | | | | | | | | | | | | |
| 5.4 | Moord(aanslag) | | | | | | | | | | | | | | |
| **6.** | **Protestactie** | | | | | | | | | | | | | | |
| 6.1 | Staking | | | | | | | | | | | | | | |
| 6.2 | Bezetting | | | | | | | | | | | | | | |
| 6.3 | Blokkade | | | | | | | | | | | | | | |

Het invullen van een Daad-Dader-Matrix is een intensief proces, zeker als alle combinaties afzonderlijk en één voor één worden geanalyseerd. Daarom kan het efficiënt zijn om in een quick scan eerst een selectie te maken. Een quick scan begint bij het 'wegstrepen' van daden die minder relevant zijn, bijvoorbeeld als blijkt dat deze daden bij deze specifieke organisatie een zodanig beperkte impact hebben dat het voor een dadertype relatief onaantrekkelijk is om tot uitvoering van die daad over te gaan. Daarbij zijn de volgende vragen relevant:

- Draagt uitvoering van de daad bij uw organisatie bij aan realisatie van de doelstellingen van een bepaald dadertype (gegeven het motief van dit dadertype)?
- Hebben deze daden zich in het verleden al (bijna) voorgedaan?
- Is er aanleiding te veronderstellen dat een dergelijke daad (momenteel) wordt voorbereid en/of zich in de toekomst zal voordoen?

| | Dadertypen | Verwarde persoon | Vandaal | Activist | Gewelddadige activist | Hacktivist | Scriptkiddie | Hacker | Gefrustreerde medewerker | Ontslagen medewerker | Lichte crimineel | Zware crimineel | Terrorist | Oneerlijke concurrent | Vijandige inlichtingendienst |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Daden** | | | | | | | | | | | | | | |
| **7.** | **Sabotage** | | | | | | | | | | | | | | |
| 7.1 | Brandstichting | | | | | | | | | | | | | | |
| 7.2 | Brandbom | | | | | | | | | | | | | | |
| 7.3 | Molest aan gebouwen, objecten, bedrijfsmiddelen | | | | | | | | | | | | | | |
| 7.4 | Fysieke vernietiging gebouwen, objecten, bedrijfsmiddelen | | | | | | | | | | | | | | |
| 7.5 | Sabotage telecommunicatie | | | | | | | | | | | | | | |
| 7.6 | High Power Microwave-wapens | | | | | | | | | | | | | | |
| **8.** | **Opblazen en beschieten** | | | | | | | | | | | | | | |
| 8.1 | Beschieting handvuurwapen (dichtbij) | | | | | | | | | | | | | | |
| 8.2 | Beschieting geweer (grote afstand) | | | | | | | | | | | | | | |
| 8.3 | Beschieting met exploderende projectielen (bijv. RPG) | | | | | | | | | | | | | | |
| 8.4 | Bombrief | | | | | | | | | | | | | | |
| 8.5 | Bompakket/rugzakbom (achterlaten) | | | | | | | | | | | | | | |
| 8.6 | Bermbom | | | | | | | | | | | | | | |
| 8.7 | Bom op persoon (zelfmoordaanslag) | | | | | | | | | | | | | | |
| 8.8 | Bomauto | | | | | | | | | | | | | | |
| 8.9 | Bomboot | | | | | | | | | | | | | | |
| 8.10 | Bomvliegtuig (van 747 tot model) | | | | | | | | | | | | | | |
| **9.** | **CBRN** | | | | | | | | | | | | | | |
| 9.1 | B/C-(poeder)brief | | | | | | | | | | | | | | |
| 9.2 | Besmetting met B/C middelen | | | | | | | | | | | | | | |
| 9.3 | Dirty bomb (nucleair) | | | | | | | | | | | | | | |
| 9.4 | Geïmproviseerd/gestolen nucleair explosief | | | | | | | | | | | | | | |
| **10.** | **Overig** | | | | | | | | | | | | | | |
| 10.1 | Nep bommelding | | | | | | | | | | | | | | |
| 10.2 | Nep poederbrief | | | | | | | | | | | | | | |
| 10.3 | Ernstige nalatigheid (verlies USB-stick, vertrouwelijke informatie) | | | | | | | | | | | | | | |
| 10.4 | Smokkel (drugs, wapens, mensen, etc) | | | | | | | | | | | | | | |
| 10.5 | Informatie-manipulatie | | | | | | | | | | | | | | |

Vervolgens kunnen dan de dadertypen worden 'weggestreept' waarvan - gegeven de kenmerken van de organisatie - weinig ongewenste daden worden verwacht. Daarbij zijn de volgende vragen per dadertype relevant:

- Waaraan ontlenen zij hun motivatie (motief)?
- Waarop zullen zij zich mogelijk richten?
- Zijn bepaalde opponenten in het verleden al dreigend geweest?
- Zouden bepaalde opponenten in de toekomst dreigend kunnen zijn?

Na deze quick scan volgt dan een meer diepgaande analyse waarin juist de combinaties van dadertypen en daden centraal staan. Daarbij zijn drie aandachtspunten van belang, die hierna worden toegelicht.

Ten eerste geeft het motief van de dader (wat wil de dader bereiken) een indicatie van de waarschijnlijkheid op een bepaalde daad bij een bepaald object. Het kan zijn dat een dadertype een bepaalde daad - bijvoorbeeld een voertuigbom - wel bij organisatie X kan uitvoeren, maar veel eerder zal kiezen voor een heel andere locatie omdat op die andere locatie de kans op doelbereik evident groter is. Met name bij de uitvoering van daden die veel voorbereiding vergen, mag ook verondersteld worden dat de opponent zorgvuldig zijn doelwit kiest.

Ten tweede kan het daarnaast zo zijn dat een dadertype - gegeven een bepaalde locatie - een daad wel kan uitvoeren, maar veel eerder zal kiezen voor een andere daad die gemakkelijk is uit te voeren of die in de uitvoering minder onzekerheid met zich mee brengt (een grotere kans van slagen heeft). Zo blijven er per dadertype maar een paar relevante daden over (omdat de andere daden wel denkbaar zijn, maar minder interessant dan de andere daden in het licht van doelbereik).

Ten derde geven de kenmerken van het dadertype een indicatie van de mogelijkheden die dit type dader heeft om de ongewenste daad succesvol uit te kunnen voeren. Bijvoorbeeld: een gefrustreerde medewerker kent het bedrijfsterrein relatief goed, heeft relatief gemakkelijk toegang tot bedrijfsonderdelen en relevante informatie en weet aan welke knoppen moet worden gedraaid om schade te veroorzaken. Dat kan worden meegewogen bij het al dan niet selecteren van dergelijke daad-dader-combinaties.

## Model 6: Checklist scenariobeschrijving

Door het toepassen van de Daad-Dader-Matrix is een selectie van relevante combinaties ontstaan. Vervolgens dienen scenario's te worden ontwikkeld waarin de daad-dader-combinaties verder worden geanalyseerd en uitgewerkt.

Een scenario bestaat uit een beschrijving van het dadertype en de daad die kan worden uitgevoerd. Hierna volgt een checklist met betrekking tot de onderdelen die in een dergelijk scenario thuishoren:

Onderdelen die relevant zijn bij een scenariobeschrijving van de dader:
- Motief (en daarmee het soort schade dat het dadertype wil veroorzaken)
- Kenmerken van het dadertype (bijvoorbeeld risicoaversiteit, bereidheid tot zorgvuldige voorbereiding)
- Toegang tot kennis
- Toegang tot middelen
- Gehanteerde (uitvoerings)tactieken

Onderdelen die relevant zijn bij een scenariobeschrijving van de daden (ook wel: modus operandi):
- Gehanteerde werkwijze door de opponent
- Middelen die de opponent nodig heeft (en de mate waarin die te verkrijgen zijn)
- Kennis die nodig is (en de mate waarin die bij bepaalde dadertypen bekend mag worden verondersteld)
- Voorbereidingen (en de wijze waarop deze kunnen worden bemoeilijkt dan wel herkend)

Overigens kan het NAVI op uw verzoek expertise inbrengen die behulpzaam is bij het construeren van scenario's. Door de samenwerking van het NAVI met onder meer de AIVD en TNO wordt geborgd dat de informatie betrouwbaar en actueel is.

## Resultaat

Na de dreigingsanalyse heeft de risicoanalist zicht op de meest relevante dreigingen (daad-dader-combinaties). Dreigingen worden als relevant beschouwd als ze voldoende realistisch zijn en een wezenlijke bedreiging vormen voor de bedrijfsmiddelen of -processen van de organisatie, dan wel voor de omgeving van de organisatie.

# 7. Stap 4: Kwetsbaarheidanalyse

## Kern van de kwetsbaarheidsanalyse

In de kwetsbaarheidsanalyse wordt de weerstand van de organisatie in kaart gebracht. Hierbij staat in het bijzonder de weerstand centraal die wordt geboden tegen de mogelijke dreigingen die in de dreigingsanalyse naar voren zijn gekomen (en uitgaande van de bescherming van de bedrijfsmiddelen en –processen en afhankelijkheden die in de afhankelijkheidsanalyse naar voren zijn gekomen). Bij weerstand kan worden gedacht aan de maatregelen die zijn genomen, bijvoorbeeld fysieke maatregelen, ICT- en informatiebeveiligingsmaatregelen, personele maatregelen en organisatorische maatregelen. Hierbij kan een onderscheid worden gemaakt tussen de permanente maatregelen en de opschalingsmaatregelen, die in werking kunnen treden bij een verhoogd dreigingsniveau (bijvoorbeeld op basis van het Alerteringssysteem Terrorismebestrijding, het ATb).

Ten behoeve van de kwetsbaarheidsanalyse worden hierna drie modellen beschreven. Ten eerste het Weerstand-inventarisatie-model. Dat model helpt om systematisch de weerstand in kaart te brengen. Ten tweede het model van de 'Business continuity factoren', dat in staat stelt om de weerstand te onderzoeken van de bedrijfsprocessen en -middelen aan de hand van de vier factoren die relevant zijn voor de business continuity, namelijk reservevoorraad, redundantie, reparatiesnelheid en vervangbaarheid. Tot slot wordt de padanalyse beschreven. Bij een padanalyse wordt vanuit een geselecteerde daad-dader-combinatie het pad met de minste weerstand gezocht.

## Model 7: Weerstand-inventarisatie-model

Eén van de belangrijkste onderdelen van de kwetsbaarheidsanalyse is het in kaart brengen van de weerstand van de organisatie in het licht van mogelijke dreigingen. Daarbij staat de vraag centraal welke weerstandsverhogende maatregelen zijn genomen (en op welke punten er mogelijk nog een gebrek aan weerstand bestaat).

Bij die inventarisatie kan onderscheid worden gemaakt in een viertal typen maatregelen (zie bijlage 5 voor de check-list aan de hand van deze vier typen):

1. **Fysieke maatregelen.** Het gaat hier onder meer om maatregelen als hekwerken, hang- en sluitwerk, compartimentering, braakwerende schillen en bergmiddelen en dergelijke.
2. **Personele maatregelen.** Het gaat hier onder meer om maatregelen bij het aannemen van personeel (antecedentenonderzoek, geheimhoudingsverklaring, psychologisch onderzoek), gedurende het dienstverband (gedragscodes, beveiligingsbewustzijn en security awareness) en bij het ontslag en vertrek van personeel (autorisaties opheffen en dergelijke). Ook gaat het hier om maatregelen inzake tijdelijk ingehuurd personeel en contractors die uitbestede taken uitvoeren (schoonmakers, onderhoudsmonteurs, et cetera).
3. **ICT- en informatiebeveiligingsmaatregelen.** Het gaat hier onder meer om maatregelen die gericht zijn op de beveiliging van ICT-processen (back-ups, virusprotectie en dergelijke). Informatiebeveiliging gaat over het borgen van de kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid.
4. **Organisatorische maatregelen.** Het gaat hier onder meer om procedurele maatregelen (omgang met bezoekers in het pand, planmatig beheer van sleutels, passen en codes, clean desk policy, veiligheidscultuur en dergelijke).

Deze vier typen maatregelen kunnen bijdragen aan de zeven beveiligingsdoelen van de organisatie, die hierna worden beschreven.

1. **Maatregelen die voorkomen** dat bijvoorbeeld gevoelige informatie openbaar wordt of kan worden. Dan gaat het bijvoorbeeld om maatregelen die zorgen dat informatie beter wordt beveiligd, dat werknemers wordt aangeleerd niet loslippig te zijn over zaken die gevoelig kunnen zijn en dat informatie niet al te snel onder het mom van publieksvoorlichting en transparantie op de website wordt geplaatst (omdat die informatie ook door kwaadwillenden kan worden gebruikt).

2. **Maatregelen die betrekking hebben op het afschermen** van het object of (digitale)systeem en het bemoeilijken van verkenningsacties. Deze maatregelen hebben als doel de potentiële dader uit de buurt van het doelwit te houden.
3. **Maatregelen die afschrikken.** Deze maatregelen hebben bijvoorbeeld als doel om de perceptie van de pakkans bij potentiële daders zodanig te vergroten dat zij zullen afzien van uitvoering van de actie.
4. **Maatregelen die tegenhouden.** Deze maatregelen hebben als doel een dader tegen te houden.
5. **Maatregelen die het mogelijk maken een incident te detecteren.** Zo kan tijdig worden ingegrepen dan wel kunnen maatregelen worden genomen om dergelijke daden in de toekomst te voorkomen.
6. **Maatregelen die de dader vertragen.** Deze maatregelen zijn gericht op bijvoorbeeld het opwerpen van verschillende barrières tot aan het doel. Dit kan zowel het binnendringen (toegankelijkheid), als het vluchten (de zogenaamde 'uitgankelijkheid') bemoeilijken.
7. **Maatregelen die een interventie mogelijk maken.** Op die wijze wordt de opponent bijvoorbeeld tijdig door een bevoegd functionaris tegengehouden.

Het invullen van het model dat hierna wordt weergegeven, kan behulpzaam zijn om de opgebouwde weerstand inzichtelijk te maken.

| | ...helpen te voorkomen dat ongewenste acties plaatsvinden | ... helpen het object af te schermen en verkenningsacties te bemoeilijken? | ...helpen de opponent af te schrikken? | ...helpen de opponent tegen te houden? | ...helpen het incident te detecteren? | ...helpen de opponent te vertragen? | ...helpen een interventie mogelijk te maken? |
|---|---|---|---|---|---|---|---|
| **Welke fysieke maatregelen...** | | | | | | | |
| **Welke personele maatregelen...** | | | | | | | |
| **Welke ICT- en informatiebeveiligings-maatregelen...** | | | | | | | |
| **Welke organisatische maatregelen....** | | | | | | | |

## Model 8: Business continuity factoren

De business continuity is voor een organisatie van groot belang. Een dag lang geen productie draaien of geen diensten leveren is buitengewoon kostbaar. Daarom dient uitval van bedrijfsmiddelen en -processen te worden voorkomen. Om goed zicht te krijgen op de weerstand die is opgebouwd om een organisatie continu te laten functioneren, dienen vier kwetsbaarheidsfactoren in kaart te worden gebracht. Dit wordt hierna geïllustreerd aan de hand van een voorbeeld waarbij een pompkamer uitvalt die olie moet toeleveren naar het bedrijfsproces.

1. **Reservevoorraad.** Als er geen olie meer kan worden toegeleverd omdat de pompkamer defect is, dan is de eerste vraag of de organisatie een voorraad heeft aangelegd nabij het productieproces die toch kan worden gebruikt (en hoe lang die reservevoorraad het productieproces op gang kan houden).
2. **Redundantie.** Zijn er meerdere pompkamers, zodat een van die kamers de functie van de defecte pompkamer kan overnemen? Zo ja, hoeveel redundantie is ingebouwd?
3. **Reparatiesnelheid.** Als er geen reservevoorraad is en als het systeem ook niet redundant is opgebouwd, dan doet zich de vraag voor of de pompkamer te repareren is en vooral: op welke termijn die reparatie uitgevoerd kan zijn.
4. **Vervangbaarheid.** Als de voorgaande borgingsfactoren geen soelaas bieden, dan doet zich de vraag voor of de defecte pompkamer te vervangen is en zo ja, op welke termijn.

Deze vragen kunnen worden geïnventariseerd voor alle belangrijke bedrijfsmiddelen en -processen van de organisatie. De volgende tabel kan daarbij worden gehanteerd:

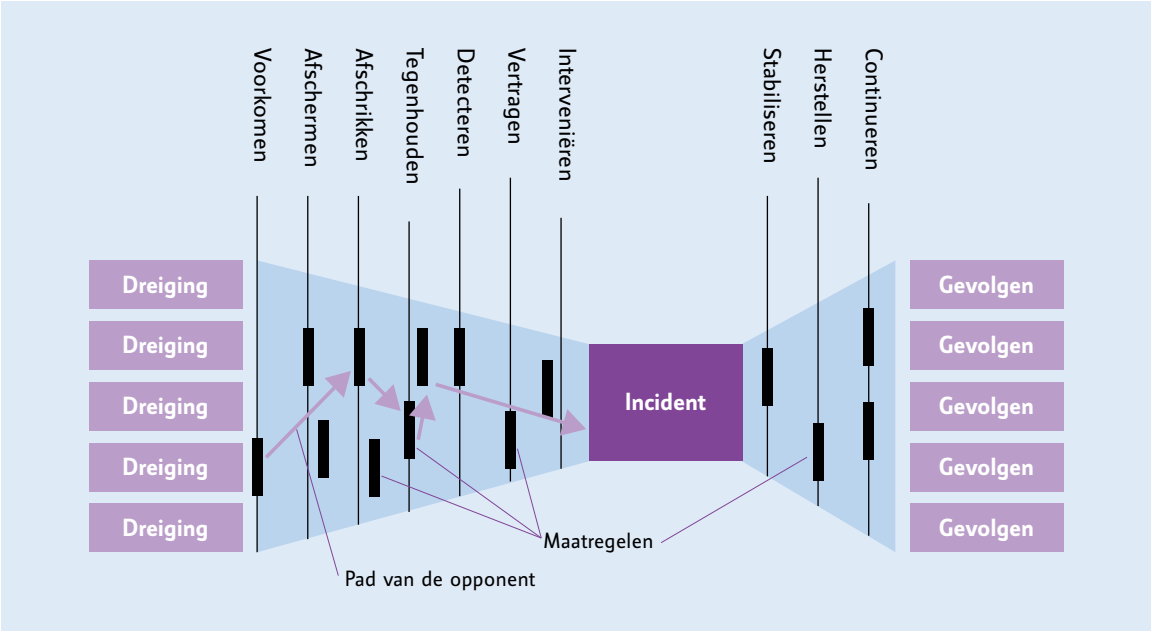
| Model 8: Business continuity factoren | | | |
|---|---|---|---|
| **Factor** | **Bedrijfsmiddel/proces 1** | **Bedrijfsmiddel/proces...** | **Bedrijfsmiddel/proces 'n'** |
| 1. Reservevoorraad | | | |
| 2. Redundantie | | | |
| 3. Reparatiesnelheid | | | |
| 4. Vervangbaarheid | | | |
| **TOTAAL-OORDEEL kwetsbaarheid** | | | |

Sommige organisaties beschikken over machines die speciaal op maat zijn gemaakt. Dat betekent dat deze machines veelal kostbaar zijn en dat de organisatie doorgaans niet meerdere machines heeft aangeschaft (redundantie). Ook kan het vervangen dan nogal wat tijd kosten, omdat de leverancier opnieuw maatwerk moet leveren. In dat geval is het dus van belang om in ieder geval goed te scoren op 'redundantie' en op 'reservevoorraad'.

## Model 9: Padanalyse

Deze analyse is met name bruikbaar voor het systematisch detecteren van zwakke plekken in de beveiliging. Bij een padanalyse verplaatst de risicoanalist zich in de opponent en zoekt de route met de minste weerstand en maximale doelbereiking.

Bij een padanalyse wordt vanuit een geselecteerde daad-dader-combinatie het pad met de minste weerstand gezocht. Als dat pad is gedetecteerd, dan wordt verder gezocht naar het pad van de op één na minste weerstand, en zo verder. Uiteindelijk ontstaat een goed beeld van de mate waarin de weerstand in staat is om bepaalde dreigingen (daad-dader-combinaties) het hoofd te bieden en waar nog de zwakke plekken zitten die mogelijk kunnen worden benut door de opponent. Een middel om blinde vlekken ten opzichte van de eigen beveiliging te detecteren, is het toepassen van een 'mystery guest'. Daarbij wordt iemand ingehuurd die als opdacht heeft om binnen te dringen. Het laten uitvoeren van padanalyses door verschillende personen afzonderlijk van elkaar is eveneens een goed middel om de weerstand te testen.



Een hulpmiddel bij het opstellen van een padanalyse is het weergegeven vlinderdasmodel. Dat model geeft inzicht in de genomen weerstandsmaatregelen ten opzichte van een dreiging. Het uitvoeren van de padanalyse en het 'intekenen' van de verschillende weerstandsmaatregelen, geeft een beeld van de sterke en zwakke plekken in de weerstand en beveiliging.

## Resultaat

Na de kwetsbaarheidsanalyse heeft de risicoanalist zicht op de kwetsbaarheid van de organisatie in het licht van mogelijke dreigingen, zowel in meer algemene zin als in relatie tot specifieke daad-dader-combinaties (die door middel van de padanalyse systematisch zijn bestudeerd). Daarnaast is inzicht ontstaan in de kwetsbaarheid van de bedrijfsmiddelen en -processen op grond van reservevoorraad, vervangbaarheid, redundantie en reparatiesnelheid.

# 8. Stap 5: Risicoweging

## Kern van de risicoweging

De risicoweging is de laatste stap in de risicoanalyse. De drie voorgaande analyses (die van de afhankelijkheden, dreigingen en weerstand) vormen de input hiervoor. De gevonden scenario's waartegen tot op heden relatief weinig weerstand bestaat, worden geschat op hun waarschijnlijkheid en op de mogelijke impact (waaronder economische schade, slachtoffers en gewonden).

Vervolgens geldt 'risico = waarschijnlijkheid x impact'. Hierdoor ontstaat een indeling van de gevonden risico's.

## Model 10: Waarschijnlijkheid-impact-analyse

Een Waarschijnlijkheid-impact-analyse is een model dat op eenvoudige wijze de waarschijnlijkheid en impact van een risico met elkaar in verband brengt. Het model wordt 'opgespannen' door twee assen: de waarschijnlijkheid dat het desbetreffende scenario zich voordoet en de impact die een scenario teweeg kan brengen.

Bij de Waarschijnlijkheid-impact-analyse worden de gevonden scenario's, die zich kunnen richten op specifieke onderdelen van de organisatie, gepositioneerd in een matrix.

*a. Schatten van de waarschijnlijkheid*

Eerst moet de waarschijnlijkheid van een scenario worden geschat. Daarvoor kan de indeling worden gehanteerd die hierna wordt beschreven, waarbij per scenario de waarschijnlijkheid kan worden bepaald.

De waarschijnlijkheidscategorieën die bovenaan staan ('niet reëel' en vlak daaronder) zijn bewust opgenomen om te borgen dat het mogelijk is om de gevonden security-risico's te vergelijken met safety-risico's (die soms in dat soort categorieën vallen, zoals een dijkdoorbraak).

| Categorie | Waarschijnlijkheid |
|---|---|
| 0 | Niet reëel |
| 1 | Niet waarschijnlijk |
| 2 | Eens op de 1 miljoen jaar |
| 3 | Eens per 50.000 jaar |
| 4 | Eens per 5000 jaar |
| 5 | Eens per 500 jaar |
| 6 | Eens per 50 jaar |
| 7 | Eens per 5 jaar |
| 8 | Eens per 6 maanden |
| 9 | Eens per maand of vaker |

Voor sommige scenario's is het relatief eenvoudig om deze indeling toe te passen, voor andere scenario's is dat juist lastiger. Het is relatief eenvoudig als bijvoorbeeld gebruik kan worden gemaakt van historische gegevens. Op grond van cijfers van bijvoorbeeld diefstal door personeel is in te schatten hoe vaak diefstal voorkomt en wat daarvan de schade is. Voor sommige scenario's is dat niet in te schatten op basis van incidentgegevens, simpelweg omdat bepaalde scenario's zich nog niet eerder hebben voorgedaan. Dat zal bijvoorbeeld gelden voor de relatief zwaardere scenario's (zoals een bomvoertuig).

**Ranking**

Wanneer er sprake is van zwaardere, minder voorspelbare scenario's kan gebruik worden gemaakt van het ranken als methodiek. Er zijn vier varianten van ranken die hierna worden beschreven (van eenvoudig hanteerbaar tot complex):

- Enkelvoudige kwalitatieve ranking. Daarbij worden daad-dader-combinaties in volgorde van waarschijnlijkheid geplaatst. Dat leidt tot een ordening zoals hierna als willekeurig voorbeeld is weergegeven (waarbij P staat voor 'probability' ofwel 'kans'): *P (diefstal medewerker) > P (computervirus hacker) > P (bomvoertuig terrorist).*
- Enkelvoudige kwantitatieve ranking. Daarbij worden niet alleen de combinaties in een volgorde gezet, maar wordt juist ook aangegeven hoeveel waarschijnlijker de ene gebeurtenis is ten opzichte van de gebeurtenis met een minder grote waarschijnlijkheid. Dat kan er bijvoorbeeld als volgt uitzien: *P(diefstal door medewerker)* ***is 3 keer zo groot als*** *P(computervirus door hacker)* ***is 100 keer zo groot als*** *P(bomvoertuig door terrorist).*
- Paarsgewijze kwalitatieve ranking. Daarbij worden alle daad-dader-combinaties onderling met elkaar vergeleken, waarbij de risicoanalist telkens moet aangeven welk van de twee scenario's meer waarschijnlijk is. Deze ranking is wat complexer dan de voorgaande, ook omdat er mogelijk inconsistenties in de beoordeling kunnen zitten doordat bijvoorbeeld risico A groter wordt geschat dan risico B, risico B groter dan risico C, maar risico C weer kleiner dan risico A. Daarom wordt geadviseerd dit type ranking alleen te gebruiken met computerondersteuning, tenzij het maximaal aantal daad-dader-combinaties zeer klein is. Overigens moeten bij vijf combinaties al tien vergelijkingen worden gemaakt, maar bij tien combinaties zelfs al 45 vergelijkingen.
- Paarsgewijze kwantitatieve ranking. In dat geval wordt bij de paarsgewijze onderlinge vergelijking niet alleen aangegeven bij welk scenario de waarschijnlijkheid het hoogst is, maar ook hoeveel maal groter die waarschijnlijkheid is. Ook dit kan vervolgens worden doorgerekend.

*b. Schatten van impact*

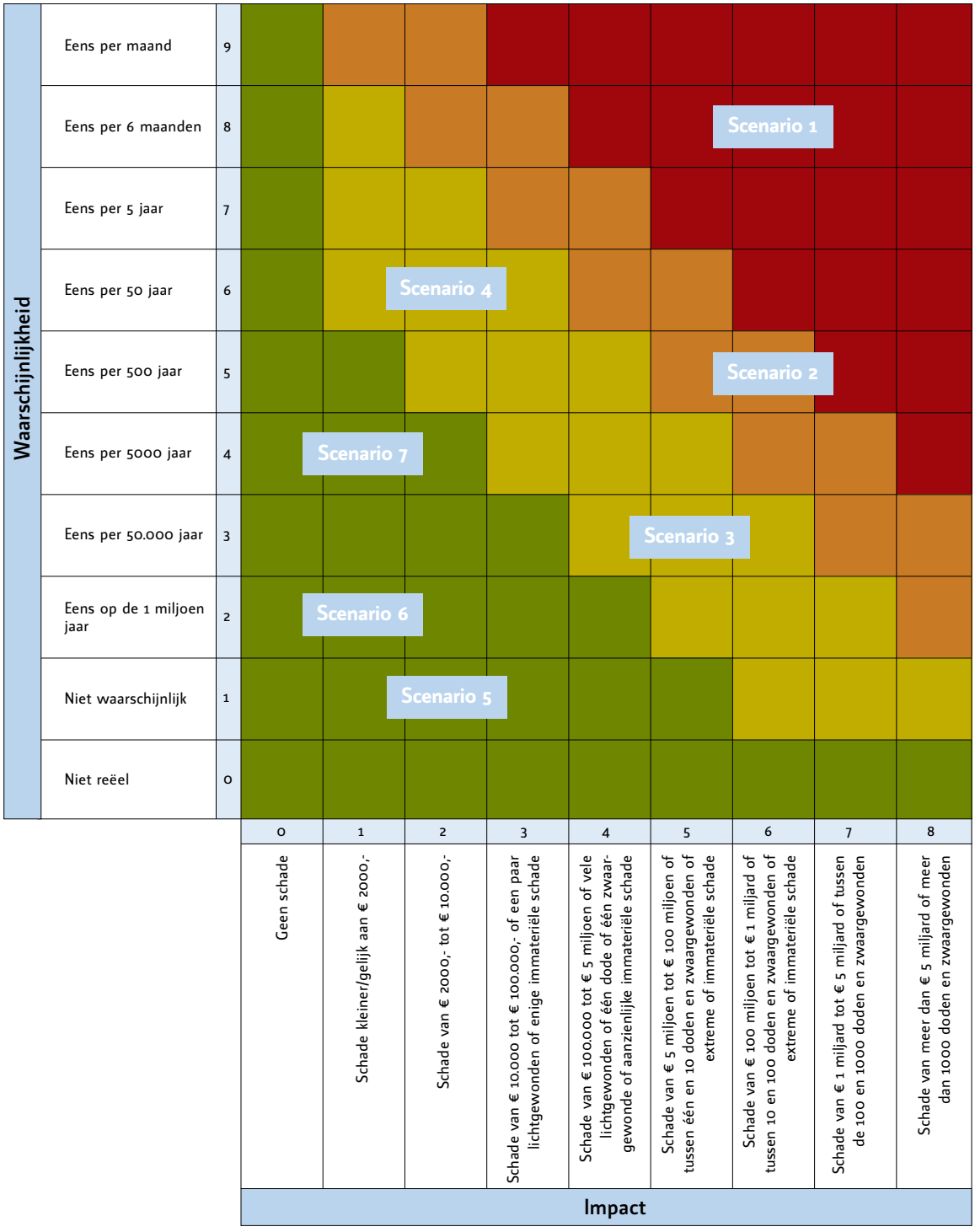
Impact kan worden uitgedrukt in geld (economische schade, maar ook milieuschade die in geld kan worden omgerekend), in slachtoffers (doden en gewonden) en in immateriële schade (zoals reputatieschade). Hierna volgt een indeling waarbij economische schade en slachtoffers in samenhang worden beschouwd:

| Categorie | Impact |
|---|---|
| 0 | Geen schade |
| 1 | Schade kleiner/gelijk aan € 2000,- |
| 2 | Schade van € 2000,- tot € 10.000,- |
| 3 | Schade van € 10.000 tot € 100.000,-<br>of een paar licht gewonden<br>of enige immateriële schade |
| 4 | Schade van € 100.000 tot € 5 miljoen<br>of vele licht gewonden<br>of één dode<br>of één zwaargewonde<br>of aanzienlijke immateriële schade |
| 5 | Schade van € 5 miljoen tot € 100 miljoen<br>of tussen één en 10 doden en zwaargewonden<br>of extreme of onmetelijke immateriële schade |
| 6 | Schade van € 100 miljoen tot € 1 miljard<br>of tussen 10 en 100 doden en zwaargewonden<br>of extreme of onmetelijke immateriële schade |
| 7 | Schade van € 1 miljard tot € 5 miljard<br>of tussen de 100 en 1000 doden en zwaargewonden |
| 8 | Schade van meer dan € 5 miljard<br>of meer dan 1000 doden en zwaargewonden |

Bij de risicoanalyse zouden de vier impactcategorieën (economie, mens, milieu, imago) ook apart kunnen worden weergegeven in plaats van gecombineerd. Echter, het gecombineerd weergeven volgens de hiervoor gegeven indeling maakt het goed mogelijk om de gevonden risico's te vergelijken met de risico's in andere sectoren, omdat daar ook deze gecombineerde indeling is gehanteerd. De gehanteerde schadecategorieën sluiten overigens ook aan bij het programma Bescherming Vitale Infrastructuur en bij de Nationale Risicobeoordeling van het programma Nationale Veiligheid.

*c. Invullen van de Waarschijnlijkheid-impact-matrix*

Vervolgens kan de Waarschijnlijkheid-impact-matrix worden ingevuld door de scenario's te positioneren.



Vanzelfsprekend bevinden de grootste risico's zich rechtsboven: grote waarschijnlijkheid, grote impact. Met name bij die risico's dient na de risicoanalyse onderzocht te worden welke aanvullende maatregelen eventueel te nemen zijn om de risico's te reduceren.

## Resultaat

Na de risicoweging heeft de risicoanalist zicht op de risico's en op de relatieve grootte ervan. Dat vormt de basis voor een discussie die nà de risicoanalyse kan worden gevoerd, namelijk de discussie over of de gevonden risico's aanleiding vormen om aanvullende maatregelen te nemen.

# 9. Na de risicoanalyse...

In de risicoanalyse zijn achtereenvolgens een afhankelijkheidsanalyse, dreigingsanalyse en kwetsbaarheidsanalyse uitgevoerd. Bij de laatste stap - de risicoweging - zijn de relevante scenario's vervolgens gescoord op waarschijnlijkheid en impact.

Dat is het einde van de risicoanalyse en tevens de start van het proces dat ná de risicoanalyse volgt: het opstellen van een beveiligingsplan waarin wordt verkend welke maatregelen eventueel genomen kunnen of moeten worden naar aanleiding van de gevonden risico's (zie ook de cyclus van het Security Management Systeem die in hoofdstuk 2 is omschreven en afgebeeld).

Er zijn vier mogelijkheden om met risico's om te gaan. Ten eerste het verminderen of beperken van risico's door het treffen van preventieve (vooraf) of repressieve (achteraf) maatregelen. Ten tweede het vermijden of opheffen van risico's door het aanpassen, innoveren (of niet meer uitvoeren) van bijvoorbeeld bedrijfsactiviteiten of bedrijfsprocessen. Ten derde het accepteren van risico's, bijvoorbeeld omdat maatregelen meer kosten dan ze opleveren. En ten vierde het overdragen van (de gevolgen van) risico's aan derden (verzekeren).

De keuze tussen deze mogelijkheden vindt plaats door een kosten–baten-analyse (KBA) uit te voeren. Dat wordt ook wel een maatregelenanalyse genoemd. In de KBA wordt geanalyseerd middels welke aanvullende maatregelen de vastgestelde risico's kunnen worden gereduceerd tegen welke kosten. Voor handreikingen met betrekking tot het uitvoeren van een KBA wordt door het NAVI verwezen naar de Handreiking Operator Security Plan. Die is - net als deze handreiking - te downloaden op www.navi-online.nl.

# Bijlage 1: Checklist voor voorbereidingsfase

Hierna wordt een checklist gegeven voor de voorbereidingsfase. Daarbij komen achtereenvolgens de afbakening, de betrokkenheid (van eigen medewerkers en van externen met bijzondere kennis of expertise) en het plan van aanpak aan de orde.

## A. Afbakening

**1 Onderwerp**

Mogelijke onderwerpen van de risicoanalyse:

- Bedrijfsonderdelen en -proces(sen)
- Vitale machines
- Gevaarlijke stoffen (calamiteus effect)
- Een of meer business units
- Een of meer vestigingen of locaties (nationaal of internationaal)
- Sector als geheel
- Intersectorale afhankelijkheid (bijvoorbeeld van elektriciteit)
- ...

**2 Scope**

Mogelijke scope van een risicoanalyse:

- Security en moedwillige verstoring (fysiek, ICT, personeel)
- Safety
- All hazards (safety en security)
- Public relations en marketing
- Informatietechnologie
- Aansprakelijkheid
- Arbo
- Milieu
- Controlling
- Disaster recovery
- Business continuity
- Integriteit
- Compliance
- ...

**3 Typen effecten en schade**

Vormen van schade die al dan niet worden meegenomen in de risicoanalyse:

- Dodelijke slachtoffers en gewonden
- Economische schade
- Milieuschade
- Politieke schade
- Imagoschade/reputatieschade
- Maatschappelijke ontwrichting
- ...

Welke schade wordt beschouwd in de risicoanalyse?

- Die van de eigen organisatie (en werknemers)
- Die van de omgeving (omwonenden)
- Die van toeleveranciers en afnemers
- ...

**4 Diepgang**

Mate van diepgang kan zijn:

- Quick-scan op hoofdlijnen
- Uitvoerige en in 'depth' risicoanalyse (vaak op deelgebieden)

**5 Periode**

Risicoanalyse frequentie:

- Eens per kwartaal
- Eens per jaar
- Eens per 3 jaar

Risicohorizon:

- Van een kwartaal tot 20 jaar

**6 Wet- en regelgeving**

Risicoanalyse opvoeren als onderdeel van te implementeren wet- en regelgeving?

## B. Betrokkenheid

**7 Interne betrokkenheid**

Van het management

- Als opdrachtgever
- Als beslissers bij tussenstappen
- Als beslissers over de follow-up na de risicoanalyse

Van medewerkers

- Als experts die kwetsbare plekken in de beveiliging kunnen aanwijzen
- Als betrokkenen die bij eventuele maatregelen hun medewerking eraan moeten verlenen (draagvlak, acceptatie)

**8 Externe betrokkenheid**

Kennis en expertise over:

- Het uitvoeren van risicoanalyses
- Security en security-management
- Reële dreigingen
- De verschillende security-domeinen zoals:
    - ICT-beveiliging
    - Fysieke beveiliging
    - Personele beveiliging
    - Organisatorische beveiliging

## C. Plan van aanpak

**9 Onderdelen van de aanpak**

- Fasering en stappen
- Doorlooptijd
- Planning
- Bemensing (interne en externe betrokkenheid)
- Tussenresultaten en -rapportages (aan wie en wanneer)
- Omgang met vertrouwelijke informatie
- ...

# Bijlage 2: Lijst van bedrijfsmiddelen en -processen, mensen en informatie

Belangen en afhankelijkheden zijn in te delen in een aantal categorieën:

- Bedrijfsprocessen
- Bedrijfsmiddelen
- Informatie
- Mensen

Deze categorieën overlappen elkaar gedeeltelijk. Zo zijn bepaalde mensen en informatie nodig om bedrijfsprocessen uit te voeren. Hierna wordt per categorie een aantal voorbeelden genoemd (niet-limitatief).

### Bedrijfsprocessen

- Productieproces
- Inkoop
- Voorraadbeheer
- Verkoop
- Marketing
- R&D (research and development)
- Transport en distributie
- Personeelszorg
- Informatiebeheer
- Facturering

### Bedrijfsmiddelen

- Machines
- Pompen
- Betalingssysteem
- Besturingssysteem
- Internettoegang
- Informatiesystemen
- Datacentra
- Kantoorruimten
- Serverruimte
- Voorraad
- Opslag gevaarlijke stoffen
- Utilities (zoals elektriciteit)
- Koeling
- Bluswater
- Wagenpark

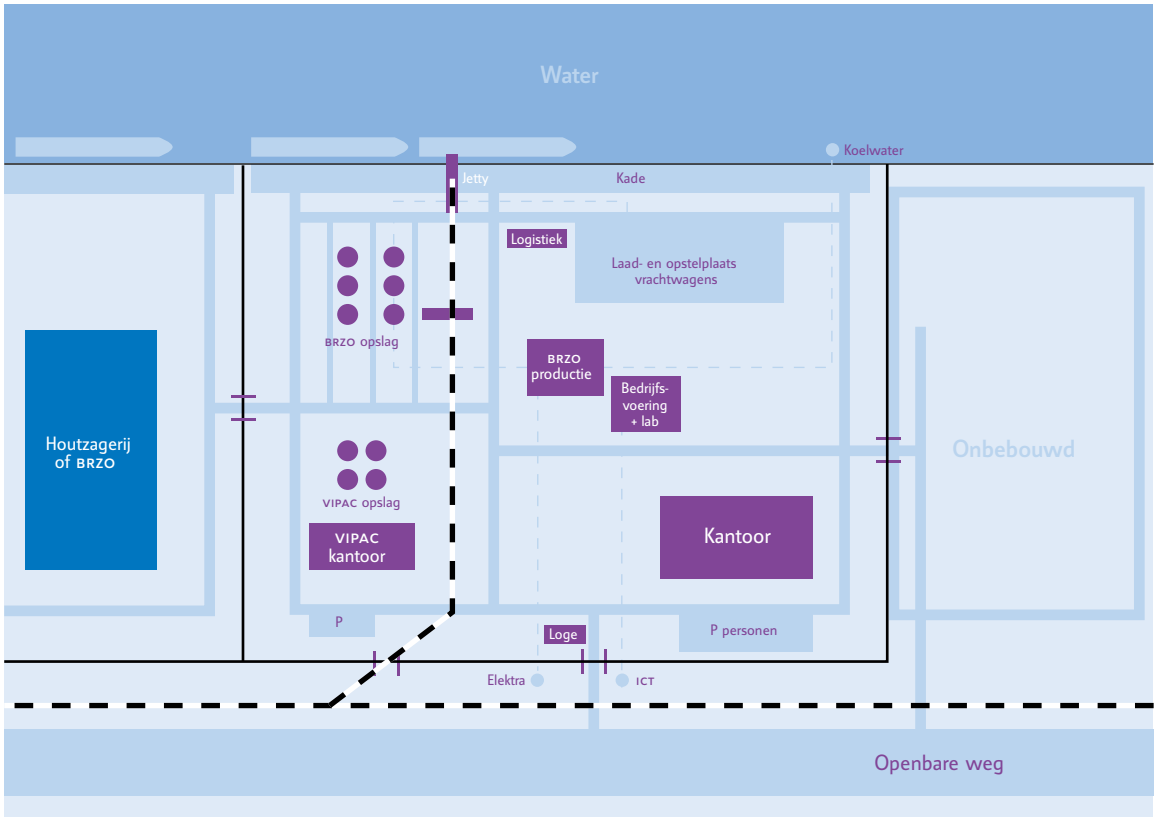
**Informatie**

- Procesautomatiseringsgegevens
- Configuratiegegevens
- Persoonsgegevens
- ICT-applicaties
- Klantrelaties (CRM-systeem)
- Financiële informatie en relaties

**Mensen**

- (Storings)monteurs
- Planners
- Directeuren
- Controllers
- Contractors
- Aandeelhouders
- Klanten
- Toeleveranciers
- Afnemers
- Bezoekers
- Buurtbewoners
- Bedrijfsvoerders / operators

# Bijlage 3: Voorbeeld schematische bedrijfsplattegrond



# Bijlage 4: Verklarende woordenlijst dadertypen en daden

### B/C-(poeder)brief

Een B/C-(poeder)bief is een brief die biologische ziektekiemen, een virus of chemische stof bevat. Wanneer een poederbrief wordt geopend, komt er een stof vrij die door middel van aanraking of inademing voor infectie of vergiftiging en mogelijk de dood kan zorgen. In oktober en november 2001 werd in de Verenigde Staten een aantal brieven met miltvuursporen (anthrax) aan personen en instanties gestuurd.

### Denial of Service (DoS)

Een actie waarbij wordt geprobeerd een computer, een systeem of telecommunicatienetwerk zo te belasten dat deze wordt uitgeschakeld en niet meer beschikbaar is voor (bevoegde) gebruikers. DoS houdt in dat een computer continu 'aangevallen' wordt door bijvoorbeeld e-mail of bepaald netwerkverkeer. Bij een Distributed Denial of Service (DDoS) wordt door een groot aantal computers tegelijk een gecoördineerde aanval uitgevoerd.

### Dirty Bomb (nucleair)

De Dirty Bomb, ofwel vuile bom, is een bom die radioactief materiaal bevat en verspreidt. Het verschil is dat de atoombom ontploft door een kettingreactie in de bom terwijl de vuile bom een conventionele springlading heeft. Er wordt dan radioactief materiaal bijgevoegd die bij ontploffing in de omgeving terechtkomt.

### Gewelddadige activist

In tegenstelling tot een activist zoekt een gewelddadige activist (extremist) op een extreme (wederrechtelijke) manier aandacht voor het eigen standpunt en/of voert hiervoor een radicale strijd. Vaak gaat het om een politieke ideologie die ver van het politieke centrum of ver buiten het centrum van de maatschappij staat. Extremisme en gewelddadig activisme zijn niet gelijk aan terrorisme, omdat er in dat geval geen aanwijzingen zijn dat een (lokale) extremist of activist als doel heeft om de bevolking angst aan te jagen of om de maatschappij te ontwrichten. Mogelijk geweld is vaak niet direct gericht tegen objecten, middelen of vitale infrastructuur maar tegen specifieke personen of (hoofd) kantoren van bedrijven en multinationals. Gewelddadige activisten kunnen individueel of in groepen opereren.

### Hacking

Tegenwoordig worden hacking en cybercrime als containerbegrip gehanteerd voor het inbreken op computersystemen of netwerken. Hacken kan plaatsvinden door een aantal (combinaties van) technieken, zoals het uitproberen van wachtwoorden, het uitbuiten van zwakheden in de programmatuur of het misbruiken van slecht geconfigureerde computersystemen.

### Hacktivisme

Het inzetten van computers en telecommunicatienetwerken om een ideologisch of politiek doel te bereiken. Aanvallen richten zich bijvoorbeeld op het beschadigen of onbereikbaar maken van internetvoorzieningen en websites.

### High Power Microwave wapens

High Power Microwave (HPM) dient als containerbegrip voor een reeks van mogelijke aanvallen middels microwave wapens gericht op elektronische apparatuur. Dergelijke wapens genereren een elektromagnetische puls (EMP) of een gerichte energiebundel (direct energy wapens). Deze wapens maken misbruik van de elektromagnetische interferentie en gevoeligheid van elektronische apparatuur. Al naar gelang het uitgezonden vermogen van dergelijke wapens kunnen storingen in de elektronische apparatuur ontstaan.

### Informatie-manipulatie (social engineering)

Informatie-manipulatie is erop gericht om vertrouwelijke of geheime informatie te verkrijgen. Bekende technieken zijn bijvoorbeeld het zich voordoen als een medewerker van de helpdesk of de automatiseringsafdeling.

### Oneerlijke concurrent

De oneerlijke concurrent als mogelijk dadertype betreft een concurrent die bijvoorbeeld op oneigenlijke wijze probeert informatie te bemachtigen. Deze informatie kan voor commerciële partijen van grote financiële en economische waarde zijn. De kans op dit gedrag is groter naarmate de concurrentie in de markt heviger is en het verlies van de één een directe relatie heeft met de (toekomstige) winst van de ander.

### RPG

RPG staat voor Rocket Propelled Grenade. Een RPG is een op veel plaatsen geproduceerde en gebruikte draagbare raketwerper die oorspronkelijk is bedoeld tegen tanks. De RPG heeft doorgaans een bereik tot ongeveer 1100 meter, maar is bij afstanden groter dan 300 meter minder accuraat.

### SCADA

SCADA staat voor Supervisory Control and Data Acquisition. De bijbehorende daad – aanval op het procesbesturings-systeem - betreft een gerichte aanval via het hacken van die systemen. Doorgaans wordt ter voorbereiding op uitgebreide schaal (openbare) informatie verzameld. In sommige gevallen worden de aanvallen over een periode 'uitgesmeerd' om de kans op detectie zo klein mogelijk te laten zijn.

### Scriptkiddie

Een scriptkiddie is een persoon die zich misdraagt op het internet, daarbij gebruikmakend van technieken en hulpmiddelen die door anderen (vaak crackers) zijn bedacht en ontwikkeld. Een scriptkiddie heeft meestal geen of beperkt verstand van de onderliggende technieken en is voornamelijk een gebruiker van andermans tools. Scriptkiddies veroorzaken veel overlast en zijn de oorzaak van veel abuse-meldingen op het internet. De groot-schalige verspreiding van veel computervirussen en -wormen kan het gevolg zijn van het werk van scriptkiddies. Dit dadertype komt echter vaak kennis en kunde te kort om daadwerkelijk een gevaar te vormen voor systemen die goed up-to-date zijn. Het doel is meestal niet om een calamiteus effect te realiseren of gevaar voor de samenleving te weeg te brengen. Echter, dat kan bij het uit de hand lopen van een bepaalde actie wel het geval zijn.

### Vijandige inlichtingendienst

Een vijandige inlichtingenorganisatie is een (overheids)organisatie die op heimelijke (clandestiene) wijze onderzoek doet in dienst van een land of organisatie. Naast inlichtingenorganisaties van overheden zijn er steeds meer private ondernemingen die actief inlichtingen verzamelen voor bijvoorbeeld multinationals. Bij veel van deze private inlichtingendiensten werken ex-medewerkers van nationale inlichtingendiensten.

### Wardiailling

Wardiailling is een wat verouderde vorm om in te breken op netwerken die stamt uit de tijd dat veel netwerkverkeer plaatsvond door middel van modems en in- en uitbelverbindingen (waarbij met name de inbelverbindingen van afstand toegankelijk konden zijn). Op die wijze kon illegaal van de verbinding gebruik worden gemaakt.

### Wardriving

Bij wardriven wordt gezocht naar signalen van draadloze netwerken en wordt gekeken in hoeverre deze netwerken beveiligd zijn. Dat gebeurt door in een auto rond te rijden (drive) en door middel van een GPS en laptop op zoek gaan naar toegankelijke of te kraken draadloze netwerken. De huidige draadloze netwerken zijn niet altijd veilig.

### Website defacing

Defacing - ook wel defacement genoemd - betreft het zonder toestemming veranderen, vervangen of vernielen van een website. Er zijn veel voorbeelden van websites die door hackers uit de lucht zijn gehaald of werden gemanipuleerd.

# Bijlage 5: Checklist weerstandsmaatregelen

In deze bijlage worden enkele maatregelen benoemd die een indruk geven van de opgebouwde weerstand bij de desbetreffende organisatie tegen moedwillige verstoring. Het betreft een niet-limitatieve lijst.

### Organisatorische weerstandsmaatregelen en -voorzieningen

- Clean desk-policy
- Vertrouwelijkheidsprocedures voor informatie
- Gesloten houden van toegangsdeuren en vluchtdeuren
- Begeleiden van bezoekers (ophalen, wegbrengen)
- Lijst van ongewenste personen bij toegangsbeheer
- Zichtbaar (beveiligings)personeel dat toezicht houdt
- Werknemers in bedrijfskleding
- Toegangscontrole via badges, portier
- Sleutelplan en sleutelbeheer
- Track & Trace: het volgen van de positie van een artikel/voertuig/persoon
- Vastleggen van belangrijke transacties en overdrachten
- Vastleggen met camerabeelden
- Brand- en sluitronden, inspectieronden
- Detectie en alarmoproep
- Alarmontvangst, -beoordeling en opstarten interventie
- Interventie tijdens een beveiligingsincident door een meldkamer (of anders)
- Bestrijden van de gevolgen van een ongewenste daad en beperken van schade
- Onderzoeken van een beveiligingsincident
- Heldere borden met gebod/verbod/bewegwijzering
- Geen borden plaatsen waar de functie van de ruimte op wordt verduidelijkt
- Sociaal toezicht door gebruikers van bedrijfsruimten
- Beperken overklimmogelijkheden bij hekwerken (door objecten die tegen/naast hekwerk zijn geplaatst)
- Verwijderen ladders, waarmee minder zwaar beveiligde gebouwgedeelten kunnen worden bereikt
- Boten, voertuigen, kranen en andere bedrijfsobjecten afsluiten
- Fotografeerverbod
- Voorkomen dat via de afvalstroom (bijvoorbeeld verpakkingen) duidelijk wordt dat attractieve goederen aanwezig zijn
- Afspraken met buurbedrijven, politie en gemeente over (opschaling) beveiligingsmaatregelen

### Personele weerstandsmaatregelen en -voorzieningen

Het betreft hier overigens maatregelen en voorzieningen ten aanzien van het personeel in drie fasen van het dienstverband: bij de indiensttreding, bij het dienstverband zelf en bij de uitdiensttreding (bijvoorbeeld als gevolg van ontslag).

- Werving-, selectie- en aannameprocedures
- Controleren CV, getuigschriften, referenties
- Antecedentenonderzoek uitvoeren
- Geheimhoudingverklaring laten tekenen
- Beveiligingsbewustzijn bevorderen (security awareness)
- Gedragscode, integriteitbeleid, integriteitstesten, drugstesten
- Functionerings- en beoordelingsgesprekken, belonings- en sanctiebeleid
- Screening of VOG op periodieke basis en/of bij doorstroom naar andere functie
- Ontslag op staande voet-procedure
- Intrekken autorisaties, (toegangs-)passen, sleutels, telefoon en dergelijke bij uitdiensttreding

- Exitgesprek met leidinggevenden en checklist laatste dag
- Monitoren gedrag na vertrek

### Fysieke weerstandsmaatregelen en -voorzieningen

- Beperkt aantal toegangen
- CCTV-toezicht (Closed Circuit Television)
- Bestrating, verlichting, kleurgebruik om gewenst ruimtegebruik aan te geven
- Gecertificeerde hekwerken/muren vensters, luiken, glasafscherming, kozijnen, hang- en sluitwerk
- Rolluiken, tralies
- Afsluitbare opbergmiddelen, kluizen (braakwerend, brandwerend)
- Zichtbeperkende maatregelen
- Plaatsen van kritische functies aan de gebouwzijde waarop geen zicht is vanaf de openbare weg
- Vastzetten en/of verankeren van een bedrijfsmiddel
- Ophijsen en/of buiten bereik plaatsen van een bedrijfsmiddel
- Toepassen van elektronische detectie op een artikel die reageert wanneer het artikel wordt bewogen of buiten een ruimte wordt gebracht
- Geen zicht op beeldschermen en op wandplaten waar mogelijk vertrouwelijke informatie op staat
- Speciale ruimten waar in vertrouwelijkheid gesproken kan worden
- Overzichtelijk terrein, zonder verstopplaatsen
- Verlichting zoals permanente verlichting, veiligheidsverlichting, schrikverlichting, geleide verlichting (verlichting om interventie te geleiden naar locatie van alarmmelding)
- (Tonen van) beveiligingsmaatregelen (camera's)

### ICT-weerstandsmaatregelen en -voorzieningen

- Toepassing van ISO/IEC 27000
- Werkstation-beveiliging, bijvoorbeeld schermbeveiliging, token, biometrie, login met wachtwoord
- Beveiligde gegevensdragers
- Hardening
- Antivirus, mallware, spyware
- Personal Firewall
- Gebruik van encryptie (data, harde schijf)
- Gecontroleerde opslag van gegevens
- Beveiligd intern netwerk ten opzichte van externe netwerken
- Autorisatie en gebruikersbeheer
- Classificatie van kritieke informatiesystemen
- Classificatie van informatie
- 24x7 Intrusion Detection System (IDS)
- IP-plannen
- Digitaal archiefbeheer