Juli 2022

Handreiking security dreigingsscenario's (petro)chemische industrie

VNCI
Koninklijke Vereniging van de Nederlandse Chemische Industrie

Inhoud

Managementsamenvatting

Grootschalige productie, verwerking en/of opslag van (petro)chemische stoffen is een van de vitale processen[1] in Nederland, aangewezen door de overheid. Daarom werd in 2008 het convenant[2] 'olie- en (petro)chemische industrie vitaal security' gesloten, dat in 2013 afliep. In dat kader zijn door de (petro)chemische industrie samen met de overheid een set standaard dreigingsscenario's ontwikkeld. Onder meer door de opkomst van moderne informatie- en communicatietechnologie en toegenomen geopolitieke spanningen zijn de 'sectorscenario's' uit 2009 opnieuw tegen het licht gehouden.

Het doel van deze handreiking is om individuele organisaties in de Nederlandse (petro)chemiesector handvaten aan te reiken waarmee zij hun eigen dreigingsscenario's en daarmee hun security managementsysteem kunnen versterken.

Uitgaande van moedwillige verstoringen wordt bij de impactanalyse gekeken naar 4 categorieën bedrijfswaarden:

1. Veiligheid en gezondheid van medewerkers en omgeving
2. Bedrijfscontinuïteit
3. Reputatie van bedrijf en/of sector
4. Directe en indirecte financiële schade

Deze handreiking beschrijft het proces dat voor een (cyber)security risico analyse kan worden gevolgd . Als eerste stap wordt een nadere toelichting gegeven op de *afhankelijkheidsanalyse*, waarbij de 'kroonjuwelen' worden geïdentificeerd en een inventarisatie van de diverse afhankelijkheden daarvan. Vervolgens wordt het dreigingslandschap geschetst, met een gedetailleerde omschrijving van daders en daden, de *dreigingsanalyse*. Om deze dreigingen in een breder perspectief te bezien dient een *kwetsbaarheidsanalyse* uitgevoerd te worden. Organisaties eindigen de actualisatie van hun dreigingsprofielen met de *risicoanalyse*; de basis van elk risicomanagementsysteem.

Startpunt van de afhankelijkheidsanalyse is het in kaart brengen van de meest relevante bedrijfsmiddelen, de zogenaamde kroonjuwelen. Daarbij kan onderscheid gemaakt worden tussen mensen, primaire en ondersteunende processen (o.a. kantoor- en procesautomatisering), hardware (o.a. fabrieken/utilities), bedrijfsonderdelen en kennis (o.a. intellectueel eigendom). Organisaties kunnen zelf een afweging maken op basis van welke criteria zij hun bedrijfsmiddelen ('assets') classificeren en dus hoe kritiek diverse bedrijfsmiddelen binnen hun operaties zijn. Als de kroonjuwelen eenmaal in kaart zijn gebracht en geclassificeerd, dienen de afhankelijkheden

[1] Vitale processen in Nederland
[2] Security convenantv

geanalyseerd te worden: onderlinge afhankelijkheden, afhankelijkheden in de leveranciers- en waardeketen en tot slot intersectorale afhankelijkheden. Het eindbeeld dat uiteindelijk ontstaat, toont een overzicht van de verschillende niveaus waarop afhankelijkheden bestaan. Dit onderscheid stelt bedrijven in staat de juiste prioritering aan te brengen.

De dreigingsanalyse is de tweede en meest omvangrijke stap van het proces en brengt de daders, daden en standaard dreigingsscenario's in beeld. In deze handreiking wordt uitgegaan van de onderstaande daders:

1. Statelijke actoren
2. Terroristische actoren
3. Criminele actoren
4. Activisten
5. Vandalen
6. Lone wolves
7. Gefrustreerde medewerkers

Genoemde daders beschikken over een breed scala aan toepasbare daden. Een overzicht van potentiële daden is als bijlage bijgevoegd aan deze handreiking. Door deze potentiële daden te koppelen aan de lijst met daders in een zogenaamde daad-dader matrix, krijgen individuele organisaties zicht in de mogelijke dreigingsscenario's voor hun organisatie. Gelet op onder meer de diversiteit van de chemische industrie en de dynamische (externe) ontwikkelingen op het gebied van (inter)nationale veiligheid is het niet mogelijk sector brede dreigingsscenario's vast te stellen. Waarschijnlijkheid en impact van de scenario's verschillen dan ook sterk per bedrijf. Voor de impactanalyse speelt vooral de aantrekkelijkheid van een doelwit ('target attractiveness') een grote rol en bij de waarschijnlijk wordt onder meer gekeken naar geografische ligging. Kijk bij het bepalen van de in te voeren maatregelen ook naar de maatregelen waarover andere organisaties verantwoordelijk zijn, bijvoorbeeld overheidsdiensten.

De een-na-laatste stap betreft het uitvoeren van de kwetsbaarheidsanalyse, waarbij onderscheid wordt gemaakt tussen weerbaarheidsvermogen en kwetsbaarheid. Het weerbaarheidsvermogen is opgebouwd uit security controls die afgestemd zijn op de risico mitigatie strategie van een onderneming. De kwetsbaarheid van een organisatie wordt in grote mate bepaald door de instandhouding en handhaving van basismaatregelen.

Sluitstuk van het proces is vervolgens de risicoanalyse. Het security risico is de uitkomst van de waarschijnlijk vermenigvuldigd met de impact (risico = kans x effect). De waarschijnlijkheid wordt bepaald door kwetsbaarheid van de organisatie en de dreiging (de intentie van de actor en zijn capaciteiten). Organisaties maken voor het inzichtelijk maken van de risico's doorgaans gebruik van een risicomatrix.

1. Introductie

1.1 Aanleiding

Grootschalige productie, verwerking en/of opslag van (petro)chemische stoffen is een van de vitale processen in Nederland, aangewezen door de overheid. Dat is een van de redenen dat security integraal onderdeel is van de bedrijfsvoering in de (petro)chemiesector. Het draagt daarmee bij aan de continuïteit van een veilige bedrijfsvoering, het terugdringen van de negatieve gevolgen van criminaliteit, het vroegtijdig signaleren van ongewenst gedrag, het beschermen van intellectueel eigendom (IP) en het versterken van de weerbaarheid tegen hedendaagse (digitale/terroristische) dreigingen.

In 2007 verscheen de eerste "Strategie Nationale Veiligheid"[3] met als doel Nederland beter toe te rusten voor het omgaan met (moedwillige) verstoringen, rampen, crises en incidenten. Hiermee moet maatschappelijke ontwrichting zoveel mogelijk worden voorkomen en/of gemitigeerd. Ook de vitale infrastructuur wordt sindsdien in samenhang met nationale veiligheid bezien, getuige het programma vitale infrastructuur, tegenwoordig bekend onder de noemer "Versterkte aanpak beschermen vitale infrastructuur"[4]. Omdat de (petro)chemie is aangewezen als vitale sector werd in 2008 het convenant 'olie- en (petro)chemische industrie vitaal security' gesloten, dat in 2013 afliep. In dat kader zijn door de (petro)chemische industrie samen met de overheid een set standaard dreigingsscenario's ontwikkeld voor de sector.

Sinds 2010 is het onderwerp (cyber)security onderdeel van het internationale Responsible Care-programma van de (petro)chemische industrie. Doel is om in de hele sector een security management systeem te implementeren die past bij de omvang en complexiteit van de bedrijven.

Onder meer door de opkomst van moderne informatie- en communicatietechnologie en toegenomen geopolitieke spanningen zijn de sectorscenario's uit 2009 opnieuw tegen het licht gehouden.

1.2 Doel handreiking

Het doel van deze handreiking is om individuele organisaties in de Nederlandse (petro)chemiesector handvaten aan te reiken waarmee zij hun security-risico's in beeld kunnen brengen op basis van voor hun relevante dreigingsscenario's en daarmee hun security managementsysteem kunnen versterken. Op bedrijfsniveau kunnen de zwaartepunten van de aanpak dan ook verschillen.

In deze handreiking wordt uitgegaan van een moedwillige aantasting van de belangen van organisaties met een significante negatieve impact op de bedrijfswaarden van een organisatie.

[3] Strategie Nationale Veiligheid
[4] Versterkte aanpak beschermen vitale infrastructuur

Bedrijfswaarden

Uitgaande van moedwillige verstoringen wordt bij de impactanalyse gekeken naar 4 categorieën bedrijfswaarden:

1. Veiligheid en gezondheid van medewerkers en omgeving
2. Bedrijfscontinuïteit
3. Reputatie van bedrijf en/of sector
4. Directe en indirecte financiële schade

2.3 Actuele sectorale dreigingsprofielen

Toen in 2009 de vorige dreigingsscenario's werden opgesteld, kende de Nederlandse overheid enkel het Dreigingsbeeld Terrorisme. Ondertussen zijn er tot maart 2022:

- 55 Dreigingsbeelden Terrorisme (DTN),
- 11 versies van het Cybersecuritybeeld Nederland (CSBN) en
- 1 Dreigingsbeeld Statelijke Actoren (DSA) verschenen.

De toegenomen (en gewijzigde) dreigingen zoals geschetst in deze beelden hebben ook hun weerslag op de (petro)chemische sector. Statelijke actoren zijn in toenemende mate assertief actief op het internationale toneel en vergaande digitalisering van industriële processen vergroot ook de impact van mogelijke digitale verstoringen. Zo blijkt ook uit de genoemde publicaties[5 6 7]:

Dreigingsbeeld Terrorisme Nederland

*"Het valt op dat **klimaatactiegroepen** in Nederland soms aansluiten bij de vreedzame demonstraties van anarchisten."*
*"In verschillende omringende landen is sprake van een opmars in links-extremistisch geweld […] Opvallend zijn aanvallen op **vitale infrastructuur** en brandstichting bij bedrijven."*

Cybersecuritybeeld Nederland 2021

*"Het afgelopen jaar zijn opnieuw wereldwijde **vitale processen** in de sectoren elektriciteit, water, olie & gas, **chemie**, transport en de zorg doelwit geweest van digitale aanvallen door criminele groepen."*

---

[5] Dreigingsbeelden Terrorisme (DTN)
[6] Cybersecuritybeeld Nederland 2021
[7] Dreigingsbeeld Statelijke Actoren 2021

Dreigingsbeeld Statelijke Actoren 2021

*"Een in het oog springend doelwit is de (digitale) **vitale infrastructuur**, waar vitale processen, diensten, toeleveranciers en de Rijksoverheid onder worden verstaan. Tegen dit type doelwit worden met name digitale sabotage (inclusief voorbereidingshandelingen) en economische instrumenten ingezet. Er is met name sprake van een toenemende interesse om kwetsbare schakels in de ketens van toeleveranciers te misbruiken. De verregaande digitalisering en afwezigheid van terugvalopties verhogen de kwetsbaarheid."*

2.4 Uitgangspunten (cyber)security aanpak (petro)chemie

De basisingrediënten van het borgen van de weerbaarheid tegen diverse (digitale en fysieke) dreigingen zijn de optelsom van hard-, soft- en mindware. Deze aanpak draagt bij aan het versterken van de bedrijfscontinuïteit en daarmee een betrouwbare, veilige en gezonde operatie van de (petro)chemische bedrijven en het vertrouwen in de sector. Daarnaast sluit deze aanpak aan bij de HSSE-risico managementaanpak binnen de (petro)chemische industrie, waarbij het gebruikelijk is security risico's in te schatten met behulp van risicoanalyses, waarbij bedrijfsveiligheidsrisico's op basis van ernst (severity) en waarschijnlijkheid (likelihood) worden geclassificeerd en gerangschikt in een zogenaamde risicomatrix.

Houd bij het bestuderen van deze handreiking rekening met de diverse codes, handreikingen en andere documenten die eerder door en voor de sector zijn opgesteld. Meest relevant in dit kader is de "Responsible Care Security Code".

Sinds 2010 is het onderwerp (cyber)security onderdeel van het Responsible Care-programma[8]. Doel is om in de hele sector een vorm van securitymanagement te implementeren die past bij de omvang en complexiteit van de bedrijven. Dit is samengevat in de *Responsible Care Security Code*[9]. Meer informatie over best practices en implementatie is te vinden in de "Responsible Care Security Code Guidance and Best Practice for the Implementation of the Code"[10].

In totaal zijn er 7 uitgangspunten gedefinieerd binnen de Responsible Care (RC) Security Code:

1. Commitment leiderschap
2. Risicoanalyse
3. Implementatie van veiligheidsmaatregelen
4. Training, ondersteuning en informatievoorziening
5. Open communicatie
6. Opvolging van dreigingen en (bijna) incidenten
7. Doorlopende evaluatie

[8] Responsible Care programma
[9] Responsible Care Security Code
[10] Responsible Care Security Code Guidance and Best Practice for the Implementation of the Code

Op basis van de Responsible Care Security Code is het van belang een periodieke review van de risico analyse uit te voeren als onderdeel van de Plan-Do-Check-Act loop.

Organisaties die nog in de beginfase staan van hun eigen security risicoanalyse worden daarnaast geadviseerd kennis te nemen van de handreiking risicoanalyse[11] van het voormalige Nationaal Adviescentrum Vitale Infrastructuur (NAVI). Hierin worden de relevante stappen van een security risicoanalyse stap voor stap toegelicht. Deze stappen vormen tevens de kapstok van deze handreiking.

Tenslotte zijn er internationale handreikingen op het gebied van security voor de (petro)chemie opgesteld; bijvoorbeeld de website van het Amerikaanse "Cybersecurity & Infrastructure Security Agency"[12].

2.5 Definities

Voor het toepassen van deze handreiking is het belangrijk een gemeenschappelijk begrippenkader te hebben. Hierna zijn de definities opgenomen die het meest van toepassing zijn voor de (petro) chemische sector. Verder verwijzen we naar (algemene) definities, die onder andere in het dreigingsbeeld Nederland zijn opgenomen[13].

Kroonjuwelen	Een kroonjuweel is een kritisch bedrijfsmiddel ('critical asset') wanneer uitval, verstoring of sabotage ervan de bedrijfswaarden aantast in een mate die groter is dan de door individuele organisaties vooraf geïdentificeerde grenswaarden. Concreet betekent dat een of meerdere gevolgen: • Aantasting van de veiligheid en gezondheid van medewerkers, omgeving en milieu; • Reputatieschade van bedrijf en/of sector; • Directe en/of indirecte financiële schade; • Verstoring van de bedrijfscontinuïteit.
Security	De beveiliging van bedrijfsmiddelen door het verkleinen van het risico op en de mate van bescherming tegen dreigingen van actoren die *moedwillig* kwetsbaarheden in een organisatie misbruiken. Deze activiteiten kunnen ongewenste impact hebben op de bedrijfswaarden (o.a. diefstal, spionage, sabotage, etc.).
Security management systeem	Het proces dat een organisatie doorloopt om grip te krijgen op security risico's.

[11] NAVI handreiking risico-analyse
[12] Cybersecurity & Infrastructure Security Agency
[13] Security definities

Dreiging	Om de dreiging te bepalen dient uitgegaan te worden van 3 elementen: intentie, vermogen en gelegenheid. Intenties en vermogen hebben betrekking op de dader, terwijl de gelegenheid wordt bepaald door de kwetsbaarheid binnen de organisatie.
Dreigingsscenario	Mogelijke scenario's waar organisaties rekening mee moeten houden bij het implementeren van hun security management systeem. Dreigingsscenario's komen traditioneel tot stand door het invullen en beoordelen van een daad-dader matrix.
Security risico	Het security risico is de uitkomst van de waarschijnlijk vermenigvuldigd met de impact (risico = kans x effect). De waarschijnlijkheid wordt bepaald door kwetsbaarheid van de organisatie en de dreiging (de intentie van de actor en zijn capaciteiten).

2.6 Scope

In deze handreiking wordt uitgegaan van dreigingsscenario's op objectniveau (bijvoorbeeld gebouw, fabriek of industrieterrein). Daarnaast is het belangrijk om rekening te houden met het sterk wisselende dreigingslandschap. Ontwikkelingen volgen elkaar snel op en daarom is een periodieke actualisatie raadzaam. Op basis van het dreigingsprofiel op organisatieniveau kan een afweging gemaakt worden over de te kiezen periodiciteit. Kijk daarbij ook naar sectorale ontwikkelingen of ontwikkelingen op nationaal niveau, zoals de Nationale Veiligheid strategie (NVS) die eind 2022 opnieuw zal worden vastgesteld.

2.7 Leeswijzer

In deze handreiking is beschreven het proces dat is gevolgd, de overwegingen en hoe bedrijven de voor hen relevante dreigingsscenario's vaststellen. Als eerste stap wordt een nadere toelichting gegeven op de afhankelijkheidsanalyse, waarbij de kroonjuwelen worden geïdentificeerd en een inventarisatie van de diverse afhankelijkheden daarvan. Vervolgens wordt het dreigingslandschap geschetst, met een gedetailleerde omschrijving van daders en daden, de dreigingsanalyse. Om deze dreigingen in een breder perspectief te bezien dient nog een kwetsbaarheidsanalyse uitgevoerd te worden. Organisaties eindigen de actualisatie van hun dreigingsprofielen met de risicoanalyse; de basis van elk risicomanagement systeem. Dit proces kan als volgt gevisualiseerd worden:

2. Afhankelijkheidsanalyse

3.1 Inleiding

Deze afhankelijkheidsanalyse is stapsgewijs opgebouwd. Allereerst dienen organisaties hun kroonjuwelen of kritische bedrijfsmiddelen in kaart te brengen. Deze vormen het uitgangspunt van de dreigingsprofielen en werken door in alle hoofdstukken van deze handreiking. Vervolgens wordt op verschillende niveaus gekeken naar de afhankelijkheden, te beginnen met de interne afhankelijkheden. Daarbij inventariseren organisaties welke onderlinge verbanden er bestaan tussen de geïdentificeerde kroonjuwelen. Vervolgens kijken organisaties voorbij hun interne processen. Een analyse van de leveranciers- en waardeketen kijkt van het beginpunt, de oorsprong van een grondstof, tot aan de uiteindelijke klant en onderzoekt in de gehele keten de mogelijke risico's voor de bedrijfswaarden. Hierbij dient onderscheid te worden gemaakt met de derde en laatste analyse van de intersectorale afhankelijkheden, ook wel cascade-effecten genoemd. Bij intersectorale afhankelijkheidsanalyses wordt voor de gehele keten gekeken naar de risico's vanuit andere aanpalende sectoren, denk daarbij bijvoorbeeld aan datacommunicatie, energie- en/of watervoorziening.

3.2 Kroonjuwelen identificeren

Kroonjuwelen worden gedefinieerd als kritische bedrijfsmiddelen die bij uitval, verstoring of sabotage ervan de bedrijfswaarden aantasten in een mate die groter is dan de door individuele organisaties vooraf geïdentificeerde grenswaarden. Dat betekent dat organisaties een classificatiemethodiek moeten hanteren waarmee ze bepalen in welke mate individuele bedrijfsmiddelen kritiek zijn voor de continuïteit van primaire processen binnen de organisatie. Daarbij dient een onderscheid te worden aangebracht tussen een vijftal categorieën van bedrijfsmiddelen:

1. Mensen
2. Processen
3. Techniek (kantoor- en procesautomatisering)
4. Bedrijfsonderdelen
5. Kennis

Organisaties kunnen zelf een afweging maken op basis van welke criteria zij hun bedrijfsmiddelen classificeren en dus hoe kritiek diverse processen en objecten binnen hun operaties zijn. Op organisatieniveau kunnen dan ook grote verschillen bestaan tussen de geïdentificeerde kroonjuwelen.

Zo kunnen organisaties met omvangrijke technologische infrastructuur zoals fabrieken een groter belang hechten aan de fysieke bescherming daarvan, terwijl organisaties die voor een groot deel van hun omzet afhankelijk zijn van specifiek intellectueel eigendom (denk bijvoorbeeld aan chemische recepturen, technologische kennis) meer belang hechten aan de bescherming van de opslag en het beheer van dit eigendom of de mensen met de meest diepgaande kennis daarvan. Tot slot dient opgemerkt te worden dat een verstoring of aantasting van de kroonjuwelen opgenomen dient te worden in de opschalingscriteria zodat de betrokken medewerkers volgens duidelijke criteria kunnen bepalen wanneer er gesproken kan worden van een calamiteit en de juiste maatregelen genomen kunnen worden. Meer informatie over de classificatie van kroonjuwelen is te vinden in de API 780 standaard over security risicoanalyses in de petrochemische sector[14].

3.3 Onderlinge afhankelijkheden identificeren

Naast het identificeren van de afzonderlijke 'kroonjuwelen' is het van belang ook de onderlinge afhankelijkheden tussen de geïdentificeerde kroonjuwelen te analyseren, omdat door de onderlinge afhankelijkheden de impactanalyse kan wijzigen. In het bijzonder relevant in dit kader zijn kantoor- en procesautomatisering. Verregaande digitalisering van primaire bedrijfsprocessen heeft geleid tot een toename van besturingssystemen. In de praktijk kan één systeem een domino-effect veroorzaken waarbij andere systemen (op zichzelf al kroonjuwelen) ook aangetast kunnen worden, hetgeen weer gevolgen heeft voor de fysieke processen. Deze onderlinge afhankelijkheden tussen kroonjuwelen en de verwevenheid van digitale en fysieke processen dienen dan ook in de security risicoanalyse meegenomen te worden.

3.4 Leveranciers- en waardeketen identificeren

Van oudsher vormen chemieclusters de ruggengraat van de Nederlandse (en internationale) chemische industrie. Voor de productie, het vervoer van chemische stoffen en het gebruik van bijvoorbeeld grondstoffen en energie zijn deze clusters onderling nauw met elkaar verbonden en wordt er intensief samengewerkt. De zogenaamde 'supply chain' kwetsbaarheden kunnen hierin een belangrijke rol spelen. Ook hier geldt dat de afgelopen jaren ketenkwetsbaarheden zijn ontstaan mede als gevolg van de toegenomen digitalisering, geopolitieke ontwikkelingen, klimaatverandering en pandemie-uitbraak (COVID-19). Toch dienen de leveranciers- en waardeketen integraal geanalyseerd te worden, zowel digitaal als fysiek. Dat is makkelijker gezegd dan gedaan en vergt maatwerk van organisaties. Kritieke schakels in de ketens hebben zelf ook meerdere afhankelijkheden waardoor een limitatieve lijst van alle schakels die de primaire bedrijfsprocessen raken niet mogelijk is.

Organisaties die inzicht willen krijgen in deze ketenkwetsbaarheden kunnen putten uit eerdere onderzoeken en analysetools. Enkele jaren geleden heeft de energiesector een methodiek

[14] API 780 Security Risico Analyse methodiek

ontwikkeld om ketenanalyses uit te voeren. Deze methodiek kan ook gebruikt of geraadpleegd worden door de (petro)chemische sector[15].

Verder kenmerkt het proces 'productie/verwerking en/of opslag (petro)chemische stoffen' zich als een bijzonder complexe keten, waarbij meerdere diensten en "utilities" cruciaal zijn voor de continuïteit van primaire bedrijfsprocessen. Bovendien zijn bij die bedrijfsprocessen uitzonderlijk veel organisaties betrokken. Denk hierbij aan organisaties die productielocaties in beheer hebben, 'contractors' voor onder meer onderhoud, IT en beveiliging. Deze complexe keten vergroot de kwetsbaarheid voor (cyber)security risico's.

3.5 Intersectorale afhankelijkheden identificeren

De vorige paragrafen hebben stapsgewijs beschreven welke afhankelijkheden voor kroonjuwelen geïdentificeerd kunnen worden. De laatste afhankelijkheid kijkt ook voorbij de leveranciers- en waardeketen en beschouwd de zogenaamde "cascade-effecten". Cascade-effecten treden op wanneer verstoringen in andere sectoren, denk daarbij aan energie, water of data-/telecommunicatie, invloed hebben op de primaire bedrijfsprocessen van organisaties in de (petro)chemische sector. Vice versa kunnen verstoringen in de (petro)chemische sector ook gevolgen hebben voor andere sectoren.

Eerdere inventarisaties van de intersectorale afhankelijkheden voor het proces "grootschalige opslag, verwerking en/of productie van (petro)chemische stoffen", onder andere uitgevoerd door de rijksoverheid, tonen een wisselend beeld van mogelijke impact. Met name de afhankelijkheid van elektriciteit en (oppervlakte)water wordt genoemd als impactvol. Ook het wegvallen van communicatie (spraak, beeld en gps) is lastig voor het bedienen van primaire processen en tijdens eventuele noodsituaties. Een verstoring in de datacommunicatie kan leiden tot verstoring in onder andere de logistieke keten, waardoor aan- en/of afvoer van grondstoffen en producten verstoord wordt.

Voorbereiden op cascade-effecten vergt scenariodenken. De meeste chemiebedrijven maken al gebruik van "maatgevende scenario's" en hebben daaraan procedures gekoppeld gericht op de veilige continuïteit van primaire bedrijfsprocessen. Dit kan ook betekenen bepaalde processen af te schalen of zelfs helemaal af te schakelen. Bij verstoringen in "utilities" wordt gebruik gemaakt van "interne noodvoorzieningen" zoals noodaggregaten die in werking treden bij het wegvallen van een of meerdere voorzieningen om continuïteit te waarborgen of een veilige en gecontroleerde afschakeling.

[15] (Cyber)security keten risico-analyse energiesector

3. Dreigingsanalyse

4.1 Trends in het risicolandschap

Mede als gevolg van maatschappelijke, geopolitieke en technologische ontwikkelingen is het risicolandschap de afgelopen jaren flink veranderd. Deze ontwikkelingen zijn van grote invloed op de actuele daders en daden waar de (petro)chemische sector mee te maken kan krijgen. Internationaal gezien is de interstatelijke competitie flink toegenomen. Vooral de grote onzekerheden van de mondiale economie maken landen kwetsbaar. Bepaalde landen kenmerken zich daarnaast door een toegenomen assertiviteit in het digitale domein. Digitale sabotage, cyberspionage, cybercriminaliteit en het aantasten van het mondiale internet zijn een aantal voorbeelden van de grote gevolgen van deze toegenomen assertiviteit. Op nationaal niveau zien we daarnaast een sterk toegenomen polarisatie, radicalisering en ongekende verwevenheid van de onderwereld met de bovenwereld, dit laatste veelal bestempeld als ondermijnende criminaliteit.

De hieronder genoemde dadergroepen beschikken over en hanteren steeds vaker nieuwe technologieën waarmee zij sneller en efficiënter te werk kunnen gaan. Te denken valt aan onder meer drones, gijzelsoftware, social engineering en blockchain.

Tot slot is het van belang kort stil te staan bij de rol van hackers. Vaak worden (kwaadwillende) hackers als een aparte dadergroep gezien, maar onderstaande opbouw van daders is gebaseerd op motieven. ‘Hacking’ is dan ook een techniek om eventueel een bepaald doel te bereiken. Hackers worden dan ook niet als aparte dadergroep opgenomen, maar kunnen onderdeel zijn van alle hierna genoemde ‘dadergroepen’.

4.2 Daders

Statelijke actoren

Wat?	Buitenlandse mogendheden die dwingende, ondermijnende, misleidende of heimelijke activiteiten ontplooien onder de drempel van gewapend conflict. Daarbij putten zij uit verschillende machtsinstrumenten, verdeeld over de categorieën militair, politiek, economisch, sociaal en informatie. Spionnen of inlichtingenofficieren in dienst van een statelijke actor zijn getraind om van buitenaf invloed uit te oefenen op een organisatie of de personen binnen die organisatie. Hierbij valt te denken aan het gebruik van. omkoping en chantage van medewerkers, vaak met geprivilegieerde toegang, te overtuigen tot een schadelijke handeling. Eigen medewerkers kunnen daarnaast ook uit eigen beweging voor of namens een statelijke actor handelen, vaak gemotiveerd door angst, vaderlandsliefde, geldelijk gewin of een combinatie van factoren.

Waarom? Statelijke actoren handelen om hun eigen (strategische) geopolitieke agenda uit te voeren. Veelal leidt dit tot directe of indirecte aantasting van nationale veiligheidsbelangen van Nederland, inclusief de belangen van de Nederlandse petrochemische sector.

Hoe? Statelijke actoren kenmerken zich door de grote verscheidenheid aan (potentiële) dreigingen en de inzet van een breed scala aan middelen. Daarbij richten zij zich onder meer op de (vitale) sectoren, waaronder de (petro)chemie, energie, defensie , maritieme sectoren (andere) sectoren met sensitieve technologieën, en hun toeleveranciers.

De recente ontwikkelingen begin 2022 in Oost-Europa, hebben kwetsbaarheden pijnlijk aan het licht gebracht, zowel fysiek (gastoevoer) als een sterke toename van cyberaanvallen.

Terroristische actoren

Wat? Personen die geweld (of de dreiging daarvan) gebruiken tegen een specifieke doelgroep of voor het veroorzaken van ernstige maatschappij ontwrichtende schade. De dreiging die uitgaat van terroristische actoren komt vaak van buitenaf, maar het valt niet uit te sluiten dat ook eigen personeel van een organisatie of samenwerking van binnenuit met een externe actor leiden tot een schadelijke handeling.

Waarom? Doelstelling is om maatschappelijke veranderingen te bewerkstelligen of politieke besluitvorming te beïnvloeden. Terroristen doen dit door angst aan te jagen door het veroorzaken van calamiteiten, waarvan calamiteiten in de (petro)chemische industrie veel slachtoffers tot gevolg kunnen hebben, of de levering van producten en diensten ernstig te verstoren.

Hoe? Er bestaat geen prototype terrorist waartegen een organisatie kan weren. De middelen die een terrorist tot zijn of haar beschikking kan hebben staan, verschillen dan ook sterk. Toch leren terroristen vaak van elkaar en vooral bij bekende terroristische groeperingen wordt zelfs samen getraind. Terroristische aanslagen in het verleden leren ons dan ook dat vooral gekozen wordt voor aanvalswapens zoals messen, pistolen en geweren of bomaanslagen. De afgelopen jaren hebben we daarnaast ook in toenemende mate aanslagen gezien waarbij ‘mobiele hulpmiddelen’ zoals voertuigen en drones werden ingezet voor het uitvoeren van een aanslag[16].

[16] Artikel droneverbod Verenigde Arabische Emiraten – Abu Dhabi

Criminele actoren

Wat? Personen die gericht zijn op het behalen van geldelijk gewin door het zich toe-eigenen van andermans bezit. Vanuit een kosten- baten analyse gebruiken criminele actoren vaak medewerkers van een organisatie om hun taken uit te voeren. Zo blijven ze zelf uit de wind en verkleinen ze de kans dat ze door de autoriteiten gepakt worden.

Waarom? Geldelijk gewin.

Hoe? Het is van belang om rekening te houden met het grote verschil in omvang bij criminele actoren. Kleine criminele actoren handelen vaak alleen of in een kleine groep, terwijl de georganiseerde misdaad zich kenmerkt door omvangrijke organisatiestructuren met veel macht en middelen. Deze laatste groep kent ook wraakacties, waarbij geldelijk gewin van ondergeschikt belang is, maar doorgaans speelt geld een primaire rol.

In het bijzonder dient aandacht geschonken te worden aan cybercriminelen die anoniem en van afstand gegevens kunnen stelen waarmee snel en gemakkelijk geld kunnen verdienen. Daarnaast zie je steeds vaker dat cybercriminelen worden gesteund door statelijke actoren. Deze ondersteuning kan indirect zijn, waarbij criminelen niet worden belemmerd door de eigen staat in het uitvoeren van hun criminele activiteiten, maar ook direct, bijvoorbeeld wanneer een statelijke actor ook de middelen levert ter ondersteuning van de criminele activiteiten.

Activisten

Wat? Personen of groepen die, om hun politieke standpunten kracht bij te zetten, zich niet laten weerhouden om middelen in te zetten die aan de wettelijke grenzen raken of daar overheen gaan. Activisten handelen vaak van buitenaf, zonder gebruik te maken van interne hulp.

Waarom? Concrete (politieke) besluiten beïnvloeden.

Hoe? Activisten maken doorgaans geen gebruik van excessief geweld. Echter, om hun boodschap kracht bij te zetten zoeken ze de grenzen van de wet op. Te denken valt aan het bezetten van gebouwen en/of toegangswegen of het aanbrengen van leuzen en andere stimulerende teksten op andermans eigendom.

Vandalen

Wat? Personen die zinloze vernielingen aanrichten. Daarbij is het van belang op te merken dat gemak een grote rol speelt. Onder invloed van verslavende middelen en/of aangemoedigd door anderen wordt vaak gekozen voor objecten die zich op dat moment binnen het gezichtsveld van de vandalen bevinden.

Waarom? Lol trappen en imponeren.

Hoe? Veelal het gebruik van het eigen lichaam, lichte wapens zoals knuppels, messen of gereedschap, graffiti of brandstichting om schade aan te richten.

Lone wolves

Wat? Personen die excessief en vaak dodelijk geweld gebruiken, in het bijzonder gericht tegen een specifiek individu of een bepaalde doelgroep.

Waarom? Lone wolves kunnen handelen vanuit psychische klachten, geloofsovertuiging of de stellige overtuiging dat een persoon of doelgroep een existentiële bedreiging vormt voor de eigen veiligheid.

Hoe? Bomaanslagen, beschieting, aanval met mes, aanrijding met voertuig

Gefrustreerde medewerkers

Wat? Personen met geprivilegieerde toegang tot terreinen, gebouwen en systemen (zoals de eigen medewerker en contractors) kunnen door verschillende oorzaken een bedreiging gaan vormen voor organisatie, medewerkers en omgeving. Dat kan gaan om frustraties in het werk, zoals gemiste promoties, problemen met collega's, botsende karakters en dergelijke, of financiële problemen. Het kan ook gaan om psychische ontregelingen: stress, overwerkt, huwelijks- of gezinsproblemen. Daarnaast bestaat de mogelijkheid dat mensen geneesmiddelen zoals psychofarmaca of drugs gebruiken. Ook overmatig alcoholgebruik kan mensen doen ontsporen. Tot slot manifesteert maatschappelijke polarisatie zich steeds vaker op de werkvloer. Te denken valt aan afnemende collegialiteit of het gebruik van bedrijfshardware voor toegang tot of verspreiding van extremistisch gedachtegoed.

Waarom? Een gefrustreerde medewerker kan vanuit verschillende motieven schadelijk handelen. Te denken valt onder meer aan: psychologische klachten, financiële problemen en/of geldelijk gewin, traumatiserende ervaringen, chantage en social engineering.

Hoe? Gefrustreerde medewerkers worden voornamelijk gekenmerkt door hun geprivilegieerde toegang tot bedrijfsterreinen, -panden en -systemen. Afhankelijk van

de motieven van deze “insiders” zijn verschillende modus operandi denkbaar. Geldelijk gewin kan bereikt worden door de diefstal en doorverkoop van intellectueel eigendom. Frustratie kan zich bijvoorbeeld manifesteren door het lekken van bedrijfsgeheimen naar media, maar ook ingrijpender zoals fysieke en digitale sabotage van primaire bedrijfsprocessen.

4.3 Daden

In een eerdere review van de mogelijke daden zoals geïdentificeerd in 2009 heeft de VNCI security werkgroep een grote hoeveelheid mogelijke daden bekeken. Een lijst met daden is opgenomen in bijlage A. Door deze potentiële daden te koppelen aan de lijst met daders in een zogenaamde daad-dader matrix krijgen individuele organisaties zicht in de mogelijke dreigingsscenario’s voor hun organisatie.

4.4 Mogelijke dreigingsscenario’s

Voor het opstellen van dreigingsscenario’s kan een individueel bedrijf de volgende stappen doorlopen:

1. Inventariseren mogelijke daders. Deze zijn hierboven genoemd.
2. Inventariseren mogelijke daden. Deze zijn opgenomen in bijlage A.
3. Samenvoegen daders aan het overzicht met daden, met als resultaat een daad-dader matrix, Deze zijn opgenomen in bijlage B.
4. Beoordelen van de daad-dader matrix waarbij wordt gekeken naar de verschillende combinaties van daders en daden en welke impact die combinaties potentieel zouden kunnen hebben op de bedrijfswaarden van organisaties. Het resultaat daarvan is een voorlopige lijst met dreigingsscenario’s.
5. Beoordelen van de mogelijke dreigingsscenario’s op waarschijnlijkheid. Scenario’s met een zeer lage tot lage waarschijnlijkheid voor het desbetreffende bedrijf vallen af respectievelijk worden niet meegenomen in de vervolgaanpak.

Wat betekent dit voor individuele organisaties?

Voor een volledige uitvoering van de vijfde stap, zoals hierboven beschreven, wordt een analyse uitgevoerd van waarschijnlijkheid en impact:

- **Waarschijnlijkheid**: Of een scenario überhaupt kan plaatsvinden. Het scenario van een bomboot valt af bij inrichtingen die niet aan of in de buurt van water liggen.
- **Impact**: Of het effect bij de betreffende inrichting zodanig groot kan zijn dat inderdaad doden en gewonden kunnen vallen, de zogenaamde doelwit aantrekkelijkheid. Als dit niet het geval is, zal de bedreiger waarschijnlijk een ander doel uitzoeken. Hierbij moet wel gekeken worden of publicitaire effecten van een scenario dusdanig groot kunnen zijn, dat zij ertoe kunnen leiden dat een scenario toch van toepassing is.

Maatregelen en afspraken die gerelateerd zijn aan desbetreffende standaard set scenario's, en die niet door het bedrijf zelf kunnen worden genomen, maar een verantwoordelijkheid zijn van bijvoorbeeld overheidsdiensten c.q. havenautoriteiten, moeten ook door het bedrijf worden meegenomen bij het bepalen of en welke maatregelen dit bedrijf neemt.

Voorbeeldanalyse waarschijnlijkheid/impact dreigingsscenario

Om bedrijven te helpen met het inschatten van de waarschijnlijkheid en de impact (het effect) wordt onderstaand dreigingsscenario ter illustratie alvast uitgewerkt. Daarbij wordt gekeken naar het scenario waarbij een statelijke actor de industriële controlesystemen van een primair proces overneemt.

- **Waarschijnlijkheid**: (geopolitieke) statelijke actoren zijn actiever en assertiever geworden gedurende het afgelopen decennia. Recentelijk is sprake van nieuwe incidenten waarbij primaire processen op afstand werden verstoord. Het is dan ook waarschijnlijk dat statelijke actoren in de nabije toekomst ook kunnen toeslaan binnen de (petro)chemische sector in Nederland. Procesautomatisering is daarnaast steeds vaker verbonden met de kantoorautomatisering, waardoor het aantal kwetsbaarheden en digitale toegangspoorten tot de systemen groter worden. Daarbij beschikken statelijke actoren over veel kennis, capaciteit en middelen. Ze gaan geduldig te werk en zijn in staat consequent op hoog niveau aan te vallen. Dit is een voorbeeld van een relevant dreigingsscenario, die leidt tot het nemen van de juiste weerbaarheids-maatregelen van de IT/OT systemen.

- **Impact**: de impact van op afstand overgenomen controlesystemen is mogelijk zeer groot. Evident is dat de financiële schade heel groot zal zijn wanneer primaire processen worden verstoord en de levering van goederen aan klanten stil komt te liggen met mogelijk reputatieschade tot gevolg. Het grootste risico schuilt echter vooral in eventuele fysieke gevolgen. Het misbruik van (petro)chemische stoffen kan leiden tot schade aan mens en milieu.

4. Kwetsbaarheidsanalyse

Zoals eerder geschetst wordt het security risico onder andere bepaald door de dreiging en kwetsbaarheid. Daarbij wordt de dreiging bepaald door de intentie van de dader en zijn capaciteiten. Echter, de eigen weerbaarheid (resp. de eigen kwetsbaarheid) heeft zeer veel invloed op zowel de intentie van de dader als zijn vermogen om te slagen. Een anekdotisch security uitgangspunt is dat 'je eigen hek altijd hoger moet zijn dan die van je buurman'. Hier zit een kern van waarheid in.

Ook al kunnen weerbaarheidsvermogen en kwetsbaarheid gebruikt worden als complementaire begrippen, er is een nuance vast te stellen. Het weerbaarheidsvermogen is opgebouwd uit security controls die afgestemd zijn op de risico mitigatie strategie van een onderneming. Kwetsbaarheid wordt voornamelijk veroorzaakt door het negeren van (cyber)security basismaatregelen , denk bijvoorbeeld aan zwak patchmanagement. Of het niet redundant inrichten van de meest essentiële processen.

Organisaties kunnen na het doorlopen van de afhankelijks- en dreigingsanalyse zelf in interne sessies hun eigen weerbaarheidsvermogen of kwetsbaarheden beoordelen. Een zeer effectief kwetsbaarheidsanalyse instrument is het "Red Teaming"[17], redelijk ingeburgerd in de cybersecurity omgeving maar ook zeer goed te gebruiken in bijvoorbeeld de fysieke security.

[17] Red teaming

5. Risicoanalyse

De doelstelling van deze handleiding is om individuele organisaties binnen de (petro)chemische sector te ondersteunen met het opzetten van hun security management systeem. Essentieel element is om mitigatie strategieën vast te (laten) stellen voor de gesignaleerde security risico's.

In de eerste stap van deze handreiking zijn de kroonjuwelen en de kritische afhankelijkheden vastgesteld. Daarna is er een overzicht gepresenteerd van voor de sector relevante daders en daden. Organisaties hebben hieruit een voor hen relevante selectie kunnen maken. Het vaststellen deze mogelijke scenario's is een essentiële stap naar het uiteindelijke security risico overzicht. Organisaties maken voor het inzichtelijk maken van de risico's doorgaans gebruik van een risicomatrix. Een voorbeeld van een risico matrix is opgenomen in bijlage C.

De kwalificatie van het security risico kan het best aansluiten bij het Enterprise Risk Management systeem dat al in gebruik is. Voor de directies of raden van bestuur is het belangrijk om de ernst van de security risico's te kunnen vergelijken met andere bedrijfsrisico's. Immers mitigatie kost tijd en geld, beiden zijn schaars.

Bijlagen

A. Daden

Afluisteren van binnenuit en buitenaf – De mogelijkheden om (van buitenaf) af te luisteren zijn flink toegenomen, bijvoorbeeld: plaatsen afluisterapparatuur, ICT sniffing, Internet of Things, smartwear/-phones, grootschalig onderscheppen (Echelon), doorbreken encryptie en straling opvangen/meelezen (Tempest).
Beschieting – Bijvoorbeeld: van grote afstand, van dichtbij, door middel van exploderende projectielen en gebruik van drones met explosieven.
Bezetting of blokkade.
Gebruik explosieven (bommen) – Bijvoorbeeld: op een persoon, in een brief, in pakket bommelding en bomvoertuigen (weg, water en lucht, inclusief drones).
Brandbom- of stichting.
Carjacking – Bijvoorbeeld: het gebruik van de auto om in te rijden op personen en objecten.
CBRN besmetting (chemisch, biologisch, radiologisch en nucleair)
Chantage – Bijvoorbeeld: dwang, omkoping en hacking.
Collateral damage (schade-effecten) – 'Onbedoelde' schade die wordt toegebracht tijdens een aanval die tegen iets of iemand anders is gericht. Denk hierbij ook aan de leveranciersketen risico's.
Compromittatie of corruptie
Diefstal – Bijvoorbeeld: gelegenheidsdiefstal, gerichte diefstal of digitale diefstal.
Gijzeling of ontvoering
Hacking – Bijvoorbeeld: gericht, ongericht, wardriving en wardialing.
Housejacking
Manipulatie – Bijvoorbeeld: social engineering, digitale manipulatie via phising, socia media (nep accounts), misbruik maken van de naam van een organisatie en 'vertrouwde' externe organisaties, zoals overheidswebsites.
Molest aan bedrijfsmiddelen, gebouwen en/of personeel
Overval
Sabotage communicatie – Bijvoorbeeld: telefoon en alarmsysteem.
Sabotage processen – Bijvoorbeeld: denial of service, distributed denial of service, HPM (High-power microwave) wapens of overname operationele systemen.
Virussen (computer) – Bijvoorbeeld: worms, tojans of ransomware.

B. Daad-dader matrix

	Statelijke actor	Terroristische actor	Criminele actor	Activisten	Vandalen	Lone wolves	Gefrustreerde medewerkers
Afsluiten van binnenuit en buitenaf							
Beschieting							
Bezetting of blokkade							
Gebruik explosieven							
Brandbom- of stiching							
Carjacking							
CBRN besmetting							
Chantage							
Collateral damage							
Compromittatie of corruptie							
Diefstal							
Gijzeling of ontvoering							
Hacking							
Housejacking							
Manipulatie							
Molest							
Overval							
Sabotage communicatie							
Sabotage processen							
Virussen							

C. Voorbeeld risico matrix

Risico Matrix

Effect	Financieel	Veiligheid & Gezondheid	Milieu	Reputatie		Waarschijnlijkheid 1 Nooit voor gekomen in chemische industrie	2 Ooit voor gekomen maar zeldzaam	3 Gebeurt 1x per jaar	4 Gebeurt enkele keren per jaar	5 Gebeurt maandelijks of vaker
	>10M	Meerdere dodelijke slachtoffers	Extreme impact	Internationale media aandacht	5 Zeer hoog					
	>1-10M	Meerdere verzuimongevallen / 1 dodelijk slachtoffer	Grote / regionale impact	Nationale of regionale media aandacht	4 Hoog					
	>100K-1M	Verzuimongeval	Lokale impact	Lokale media aandacht gedurende meerdere dagen	3 Gemiddeld					
	>10K-100K	Medische ingreep	Beperkte impact	Lokale media aandacht	2 Laag					
	<10K	EHBO	Zeer beperkte impact	Alleen interne communicatie	1 Zeer laag					