Evaluatie Securitycontroles Bevb

2019

Versie

Datum	13 januari 2020
Status	Definitief

Colofon

ILT
Keten Gevaarlijke Stoffen en Organismen

Contactpersoon F.J. Huisman
coördinerend/specialistisch inspecteur

fred.huisman@ILenT.nl

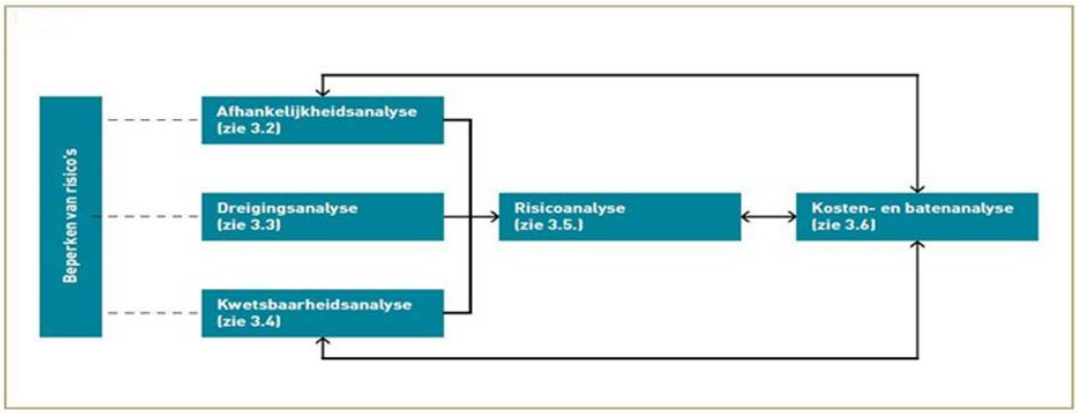
Versie

Opdrachtgever Petra Doornhof KGSO/H-RB
Auteur Fred Huisman
Projectnummer

Inhoud

Inleiding

In het najaar 2019 zijn Securitycontroles uitgevoerd bij een 5-tal buisleidingenexploitanten, vallend onder het Bevb, en één beheerder van een buisleidingstraat. Dit type controle werd voor het eerst uitgevoerd bij Bevb-exploitanten en had een inventariserend karakter. In voorliggend rapport staan de bevindingen samengevat en een evaluatie gericht op mogelijke wensbaarheid voor Security-controles in de toekomst.



1 De aanpak, algemeen

1.1 Securitymanagement, algemeen

Securitymanagement heeft te maken met het borgen van continuïteit van de onderneming (assetmanagement) respectievelijk de vitale infrastructuur van NL. En als beperking van gevaren voor de omgeving, die kunnen ontstaan als gevolg van aanslagen en sabotage (externe veiligheid, maatschappelijke ontwrichting). Securitymanagement gaat tenminste over de volgende elementen[1]:

1. Een vastgesteld Securitybeleid.
2. Risico-identificatie en –analyse (risicomanagement).
3. Securitymaatregelen en voorzieningen.
4. Afspraken over de interne en externe Securityorganisatie.

Organisatorische en personele beveiligingsmaatregelen worden samen met bouwkundige en elektronische voorzieningen (waaronder ICT) ingezet om de Security doelstellingen te bereiken. Dat maakt Securitymanagement een complex vak. Het vraagt om een gestructureerde, planmatige en *systematische* aanpak. Door het inrichten en onderhouden van een *Security management*systeem wordt het mogelijk de Security doelstellingen efficiënt en effectief te realiseren.

Risicomanagement
Om een goede risicoanalyse te kunnen uitvoeren is kennis en informatie nodig over het bedrijf, over concrete en potentiële dreigingen én over maatregelen die de weerbaarheid van een bedrijf verhogen. Doel van de risicoanalyse is om in te spelen op ernstige risico's van nu en in de nabije toekomst.
Drie belangrijke aspecten dragen bij aan de risico's die een bedrijf loopt, te weten de onderwerpen:

a) Bedrijfsbelangen.
b) Dreiging.
c) Kwetsbaarheid.

Ad a) De bedrijfsbelangen betreffen de vitale bedrijfsprocessen en cruciale onderdelen van het bedrijf. Deze belangen, waarvan het bedrijf afhankelijk is voor het bereiken van zijn doelstelling, moeten beschermd worden om ernstige bedrijfseconomische of maatschappelijke schade te voorkomen.
Ad b) De dreiging hangt af van de mogelijkheden van potentiële daders (capability) en de mate waarin zij bereid zijn om hun daad uit te voeren (intent). Tijdens de risico-inventarisatie en –analyse zal deze dreiging in kaart moeten worden gebracht. Daarbij is de doelstelling het meten van de bereidheid en de mogelijkheden van de daders en deze vervolgens te rangschikken op de mate van gevaar die zij voor het bedrijf opleveren.
Ad c) De kwetsbaarheid hangt af van de mogelijkheden die de omgeving deze potentiële daders biedt. De weerbaarheid van een bedrijf (getroffen beveiligingsmaatregelen) is in dit kader belangrijk.
Let op: Wanneer men zich echter op risico's oriënteert - dus naast de dreiging, de kwetsbaarheid en het belang in de overwegingen meeneemt - is het niet uitgesloten dat men ondanks een lage dreiging grote risico's moet vaststellen.

[1] **Risicoanalyse Security, schematisch (https://www.Security-kaders.nl)**

1.2 Securitymanagement, “de eisen”.

1.2.1 Wettelijke basis

De wettelijke basis voor Securitycontroles is terug te vinden in:

- ✓ Bevb, namelijk art. 4 (zorgplicht) en art. 10 (ongewone voorvallen).
- ✓ NEN 3655, namelijk in art. 5.4 (RI&E, bewust uitgevoerde externe verstoringen).

1.2.2 Securitymanagement

Er zijn diverse managementsystemen die bedrijven moeten ‘wapenen’ tegen ongewenste beïnvloeding van buitenaf. Bijvoorbeeld:

- ➢ ISPS: International Ship and Port facility Security Code met minimumeisen voor beveiliging van schepen, havenfaciliteiten en overheidsinstellingen. Geldt met name voor locatie waar een wal-schip connectie is (schip ligt aan de kade). Vanuit IMO (international maritime organization) verplicht.
- ➢ ISO-NEN-IEC 27001 (2016): internationale standaard voor informatiebeveiliging. Denk aan bescherming van persoons- en bedrijfsgegevens, bescherming tegen hackers, en het weerbaar zijn tegen calamiteiten (incl. cyberaanvallen). Op vrijwillige basis.
- ➢ ISO-NEN 22301: Business continuity management system (BCMS) ter bescherming tegen, verkleining van de kans op, voorbereiding op, reactie op en herstel van verstorende incidenten wanneer deze zich voordoen. Op vrijwillige basis.

1.3 Fysieke Security versus Cyber Security

De door de ILT uitgevoerde controles zijn vooral gericht op de maatregelen die op het fysieke en organisatorische vlak liggen. Niet op het gebied van Cyber Security, ondanks dat Cyber-Security inbreuken steeds meer voorkomen (Hackers, Ransom-software).
Weliswaar staat er in de vragenlijst een vraag over de weerstand tegen hackers (SCADA-systemen) maar de expertise bij de ILT-inspecteurs van het Bevb-toezicht (KGSO/RB) is onvoldoende om over Cyber-Security een oordeel te geven.
Kortom: *het gaat hier dus niet om Cyber-Security.*

1.4 Doelstelling(en) ILT-controles

Het doel van de Security-aandacht vanuit de ILT is om de bewustwording bij de exploitanten voor Security te beoordelen en te bevorderen. Veelal denkt men al voldoende vanuit Safety te hebben gedaan en daarmee ook Security af te dekken. Maar dat is een te snelle redenatie. Security-aandacht vraagt om een geheel andere optiek dan Safety-aandacht. Het gaat om zaken als afhankelijkheid, kwetsbaarheid met dreiging vanuit potentiële, bewuste en kwaadwillende beïnvloedingscenario’s van buitenaf. En dat behoeft dan ook andersoortige aandacht en maatregelen. Kort samengevat zijn de doelen:

- ✓ Bewustheid m.b.t. Security-scenario’s
- ✓ Vastleggen van de weging van assets op afhankelijkheid, kwetsbaarheid, dreiging.
- ✓ Afscherming van gevoelige informatie tegen inzage door onbevoegden.

1.5 De ILT-audits, de uitvoering

De ILT-audits vonden zoals al aangegeven bij 5 exploitanten en 1 beheerder van een leidingstraat. De audits waren inventariserend van karakter, gericht op een

algemeen beeld van de Security-aanpak bij/voor de exploitanten. Dit om een basis te leggen voor een mogelijke vervolgaanpak vanuit de ILT, in 2020 (e.v.). Beeldvorming vond plaats op basis van interviews. Verificatie, door het inzien van stukken, heeft slechts beperkt plaatsgevonden. Verificatie door het beoordelen van praktijksituaties heeft in deze fase nog geheel niet plaatsgevonden.

De gehanteerde criteria om tot een keuze te komen van te controleren exploitanten/beheerder zijn de locaties waar:

- ✓ Vooral vervoer plaatsvindt van stoffen die bij diefstal eenvoudig doorverkocht kunnen worden. Motivatie: diefstal.
- ✓ Vervoer van acuut toxische stoffen met hoge gevaarzetting (bij lekkages) voor mensen. Motivatie: terrorisme, maatschappelijke ontwrichting.
- ✓ Vervoer van gevaarlijke stoffen via bovengrondse leidingdelen die eenvoudig te traceren zijn voor kwaadwillenden. Motivatie: sabotage, terrorisme, maatschappelijke ontwrichting.

1.5.1 Behandeling vertrouwelijkheid

Vanwege vertrouwelijkheid zijn een aantal keuzes gemaakt. Deze zijn:

a) De namen van de bezochte exploitanten/beheerder worden in deze rapportage niet vermeld.
b) Documenten met informatie over Security bij/voor exploitanten krijgen de rubricering “Departementaal Vertrouwelijk”.
c) De ingevulde vragenlijsten/rapportages worden alleen “encrypted” ter beschikking gesteld aan de betreffende geauditeerde exploitant/beheerder.
d) Op de O-schijf en in Holmes worden alleen ‘encrypted’ documenten geplaatst. Dit voorkomt inzage door onbevoegden.

1.6 De auditrapportage

De vooraf toegezonden vragenlijst werd aangevuld met de bevindingen van de ILT. Daarmee ontstaat de auditrapportage (op basis van ‘vraag/antwoord’).
Deze rapportage werd na de ILT-audit eenmaal ter controle op feitelijke onjuistheden aangeboden aan de betreffende exploitant/beheerder (encrypted, wachtwoord via sms).
In de eerste audits werd de definitieve rapportage digitaal (encrypted, wachtwoord via sms) en per post (aangetekend, dubbele envelop) verzonden aan desbetreffende exploitant/beheerder. Later vond verzending slechts digitaal (encrypted, wachtwoord via sms) plaats. Dit omdat het per post verzenden omslachtig was en onveiliger leek.

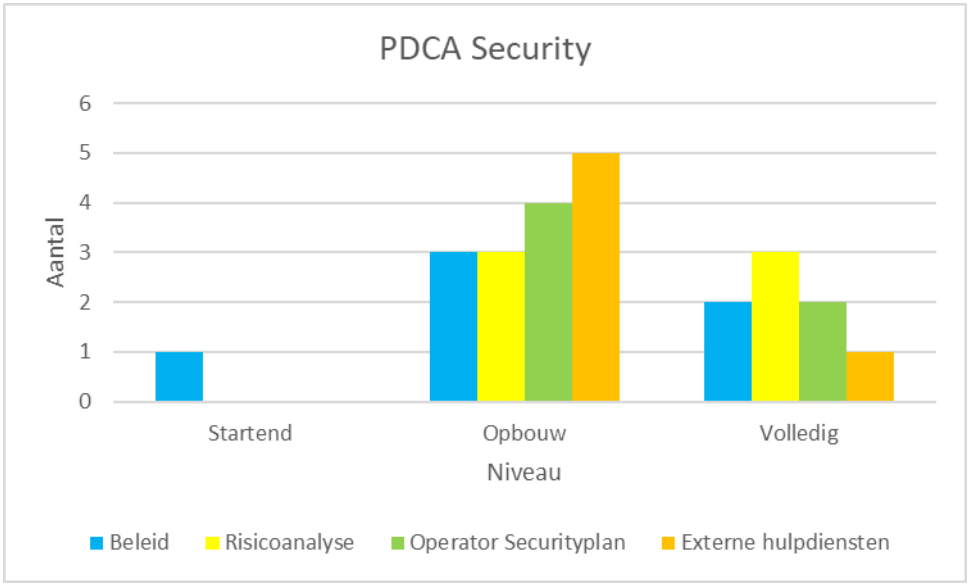
2 Resultaten

2.1 Algemeen, overall beeld

De PDCA voor Security bevat enkele belangrijke onderdelen. Deze zijn:

- Securitybeleid
- Risicoanalyse
- Operator Securityplan
- Externe hulpdiensten

Het overall beeld uit de 6 inventariserende audits, is hieronder grafisch weergegeven. Een enkel punt zit nog op start/basisniveau, het grootste deel is “Verder in Opbouw” en (nagenoeg) op het niveau “Volledig”.



In volgende paragrafen staat meer achtergrondinformatie over deze onderdelen.

2.2 Securitybeleid

Eisen:
Een organisatie formuleert beleid om haar doelstelling te kunnen realiseren. Men heeft een bepaald doel voor ogen. Is door het bedrijf onderkend dat Security inbreuken kunnen plaatsvinden? En is beschreven hoe de organisatie Security op een doelmatige, structurele, integrale en efficiënte wijze zal inrichten ter bescherming tegen kwaadwillig menselijk handelen?

Resultaten:
Bij 1 exploitant was het Securitybeleid nog op het niveau ‘start/basis’. Het beleid had daar nog grotendeels een ‘Safety karakter’. Bij 3 exploitanten was het al ‘verder in opbouw’ en bij 2 exploitanten was dat geheel of nagenoeg ‘volledig’.

Opvallende zaken Securitybeleid:

a) Het opnemen van een expliciete doelstelling gericht op Security was is enkele gevallen niet aanwezig.
b) Het aanwijzen van een verantwoordelijke persoon voor Security vond overal plaats. Soms duidelijk, bijvoorbeeld met Security in de functietitel en afdelingsnaam, en soms minder duidelijk.
c) In de managementreview (directiebeoordeling) was Security in een aantal gevallen geen vast onderdeel.
d) In meerdere gevallen was er sprake van een assetmanagementsysteem met daarin aandacht voor Security.
e) In het geval van een kadegrens van een aansluitende inrichting was ISPS binnen de bedrijfsvoering als beveiligingsnorm bekend.
f) Het aan ingehuurde aannemers meegeven van afdoende aandacht voor Security kan beter.
g) In het geval van een ingehuurde provider voor het onderhouden van het VBS, was er bij de exploitant onvoldoende parate kennis over de Securityaanpak.

2.3 Risicoanalyse Security

Eisen:
De risicoanalyse, bij de exploitanten veelal bekend als RI&E, is een weging van de kansen en gevolgen van een ongewenste gebeurtenis. Het leidt tot inzicht in de impact en waarschijnlijkheid van die gebeurtenis en in de weerbaarheid van een organisatie tegen bedreigingen van vastgestelde belangen, uitval en verstoringen van kritische processen. Die weerbaarheid wordt afgemeten aan de maatregelen die zijn genomen om de waarschijnlijkheid op verstoring te verminderen en de gevolgen beheersbaar te maken. Uiteindelijk komt uit de analyse een risicobeeld dat ertoe kan toe leiden om extra maatregelen te treffen.

Een Security-risicoanalyse kan worden opgedeeld in onderdelen. Hier is de score verdeeld over deze onderdelen:

Onderdeel	Startend						Verder in opbouw						Volledig					
Voorbereiding																		
Afhankelijkheidsanalyse																		
Dreigingsanalyse																		
Kwetsbaarheidsanalyse																		
Risicoweging																		

Bij alle onderzochte exploitanten/beheerder was de aanpak van een risicoanalyse bekend. Veelal via de RI&E van de Safety benadering waaraan Security in meer of mindere mate was toegevoegd.
Het beeld uit de audits daarover was dat de voorbereiding en de risicoweging over het algemeen goed bekend en doorgevoerd was.
Het maken van een dreigingsanalyse, kwetsbaarheidsanalyse en (in wat mindere mate) een afhankelijkheidsanalyse was vaak minder expliciet uitgevoerd.

Opvallende zaken bij de risicoanalyse Security:

a) De RI&E-aanpak bevat vaak ook Security. In een enkel geval was er ook sprake van een 'Business-continuity-plan' en een 'Threat-landscape' om risico's 'te managen'.
b) Dreigingscenario's, zoals terrorisme en diefstal, worden benoemd en zijn kort beschreven. Soms was dat maar voor 1 scenario omdat de kans op andere scenario's laag werd ingeschat. Soms ook werden meerdere (tot 4 stuks) scenario's beschreven, ook als de kans vooraf als laag werd ingeschat (=beter).
c) In enkele gevallen was de aanpak uit ca. 2010 van het landelijke Securityproject "VITAAL" (en ondersteuning vanuit toenmalige NAVI) nog duidelijk zichtbaar. De Security-aanpak oogde daar beter.
d) Vaak worden afsluiter- en boosterstations als belangrijke en kwetsbare onderdelen van de buisleiding onderkend. En krijgen daarbij Security aandacht.
e) Het vastleggen en afschermen van gevoelige informatie over scenario's, afhankelijkheden, kwetsbaarheden en dreigingen vindt veelal onvoldoende plaats. Vaak kon alle personeel deze informatie inzien.
f) Het koppelen van Securitymaatregelen aan dreigingscenario's vindt veelal nog onvoldoende expliciet plaats. Daderprofielen, motivatie en middelen (en bijhorende pad-analyses) zijn nog niet beschreven.
g) In een leidingstraat was sprake van een eigen aanpak van inschatten domino-effecten. Dit gebeurde om een betere risicoanalyse te kunnen maken.

2.4 Operator Securityplan

Eisen:
Een operator Security plan of beveiligingsmaatregelenplan geeft aan welke operationele beveiligingsmaatregelen gelden om gedefinieerde bedrijfsbelangen tegen benoemde dreigingen te beschermen. Het betreft beveiligingsmaatregelen van bijvoorbeeld fysieke, personele, organisatorische en logische (ICT) aard. Securitymaatregelen kunnen in routinematige situaties en in bijzondere dreigingsituaties optreden. Daarnaast is vastgelegd op welk wijze deze maatregelen beheerd worden.

Resultaten:

- 4 exploitanten op het niveau 'verder in opbouw'
- 2 exploitanten (nagenoeg) 'volledig'.

Securitymaatregelen voor de leidingen en bijbehorende componenten zijn er wel. De koppeling van maatregelen met dreiging scenario's kan beter. Daarbij blijft de vraag onbeantwoord of de maatregelen terecht resp. voldoende zijn.
En de afscherming van deze (voor kwaadwillenden interessante) informatie schiet tekort.

Opvallende zaken:

a) Vaak zijn Security-maatregelen (fysiek en organisatorisch) doorgevoerd, zoals visuele trajectcontroles en het plaatsen van hekken en camera's, bijvoorbeeld bij stations
b) Een totaaloverzicht van Securitymaatregelen was veelal niet aanwezig. Wel in deeloverzichten (bijv. t.b.v. planning van onderhoud of controles).

c) In het geval van een ingehuurde provider voor het onderhouden van het VBS, was er bij exploitant onvoldoende parate kennis over de Securityaanpak.
d) Afscherming van de informatie van deze deeloverzichten was onvoldoende. Dit geldt voor de inzage binnen het bedrijf (iedereen kan alles inzien?) en vooral ook als werk (onderhoud) was uitbesteed aan derden.
e) Koppeling van maatregelen met een specifiek beveiligingsdoel/ dreigingsscenario ontbrak vaak.

2.5 Externe afstemming, hulpdiensten

Eisen:
De interne beveiligingsmaatregelen van een bedrijf zijn afgestemd met de, op de beveiliging gerichte maatregelen van externen. Zoals de betreffende gemeente(n), de regiopolitie en eventueel andere partners/stakeholders (bijvoorbeeld externe beveiligingsorganisaties). Deze afstemming is vastgelegd.

Resultaten:
Contacten met hulpdiensten zoals een ingehuurde beveiligingsfirma en de politie (wijkagent) vindt over het algemeen regelmatig plaats. Daarbij voert het aanpakken/behandelen van Safety incidenten de boventoon. Het aanpakken/behandelen van de effecten van Security incidenten loopt daarin mee. Contacten met AIVD (over dreigingen) vindt slechts in enkel gevallen plaats. Het beoefenen van Security scenario's, dat wil zeggen in preventieve zin (het voorkómen van Security-incidenten), vond niet plaats.

Opvallende zaken:
a) Contacten zijn er met politie/wijkagent en de eigen (vaak ingehuurde) beveiliging. Soms structureel en soms incidenteel.
b) Minder contact is er met veiligheidsregio's en AIVD.
c) Vaak wordt voor externe ondersteuning teruggevallen op het bellen van 112 (met aansluitend maatwerk ter plaatse).
d) Securityoefeningen zijn er soms op ICT-gebied (Cyber-Security) maar niet op technisch gebied. Wel Safety oefeningen maar geen beoefening van Security scenario's, gericht op het voorkómen van Security incidenten.
e) In enkele gevallen zijn er concrete Security-incidenten geweest waardoor beoordeeld kon worden hoe de samenwerking loopt. Dat liep goed.
f) Afspraken met externe hulpdiensten (zoals politie, veiligheidsregio) over de wijze waarop wordt gereageerd bij de verschillende scenario's zijn niet vastgelegd. In een enkel geval geldt dit ook voor het ingehuurde beveiligingsbedrijf (alleen responstijden).

3 Vastleggen resultaten

Zoals al aangegeven kunnen de audit-resultaten vertrouwelijke gegevens bevatten. Daarom worden er geen papieren rapportages binnen de ILT opgesteld/bewaard. De rapportages zijn digitaal en encrypted. Het wachtwoord daarvan is alleen binnen het betrokken toezichtteam (KGSO/RB/buisleidingtoezicht) bekend. Daardoor kunnen ook ICT-ondersteuners van IenW/ILT geen toegang krijgen tot de resultaten.

Vastleggen van de resultaten in Holmes vindt plaats op twee wijzen:

1. Het ‘encrypted’ rapport in de map documenten.
2. Een summier ingevulde vragenlijst zonder inhoudelijke info.

In de bijlage staat een voorbeeld van een ingevulde vragen uit Holmes.

4 Evaluatie en conclusies

4.1 Evaluatie werkwijze

De werkwijze van de inventariserende audits werkte over het algemeen goed.

a) De vooraf toegezonden vragenlijsten waren bij alle exploitanten/beheerder goed bekeken.
b) Het doorlopen van de vragen verliep soepel en de benodigde tijd was 1,5-2 uur.
c) Een nadere beoordeling of vragen anders geformuleerd kunnen worden of achterwege kunnen blijven wordt wel voorgesteld.
d) Het encrypted toezenden van de resultaten met daarbij een wachtwoord was wat lastig maar werd door betrokkenen nodig geacht. Het werkte op zichzelf goed.
e) In 5 gevallen werd ook het concept opgestuurd ter beoordeling op feitelijke onjuistheden. Een reactie daarvan was vaak al binnen 1 week terug.
f) Van de exploitanten wordt verwacht dat de bij Security betrokken personen op integriteit zijn beoordeeld. En kan immers kennisgenomen worden van gevoelige informatie. De vraag ligt in principe ook voor bij de ILT of betrokken ILT-personeel voldoende op integriteit is gescreend.
    - De vraag ligt voor of ILT-personeel dat betrokken is bij Securitycontroles daarvoor extra gescreend moet worden.
g) Het toezenden van een papieren exemplaar vond tweemaal plaats maar werd daarna niet meer gedaan. Dit omdat:
    - De toegevoegde waarde (naast een digitaal exemplaar) minimaal lijkt.
    - De exploitanten vonden het overbodig.
    - Het omslachtig was voor de inspecteur (extra briefjes).
    - Toch een papieren versie, dat lastig te beveiligen is.

    De vraag is echter wel in hoeverre de directie van een bedrijf kennisneemt van het feit dat er een Securitycontrole heeft plaatsgevonden en wat de resultaten daarvan waren. Hopelijk gebeurt dat sowieso in de directiebeoordeling.

4.2 Conclusies

Qua aanpak werkte de aanpak met de inventariserende vragenlijsten goed.
Uit de auditresultaten (H3) blijkt het dat de Security aanpak bij een aantal exploitanten op punten verbeterd kan worden. Gelet op de huidige (bij ILT bekende) Security incidenten (diefstal) is er daarbij nog geen reden tot grote zorg. Maar een hogere bewustheid dat Security-scenario's niet alleen theoretisch zijn lijkt bij een aantal exploitanten op zijn plaats. Een beter geborgde weerstand tegen Security incidenten, ter voorkoming van grote risico's in de toekomst is in meerdere gevallen nodig. Daarbij ligt het voor de hand de verbeterde zorg voor Securitymanagement onder te brengen in de reguliere VBS-aanpak bij exploitanten.

5 Aanbevelingen

Aanbevolen wordt om de inventariserende Security-audits voort te zetten bij de overige exploitanten. Daartoe worden de volgende stappen voorgesteld:

a) Beoordelen of de vragenlist op details moet worden aangepast
b) Bespreken resultaten met de branchevereniging Velin die in het verleden al eens aandacht van haar leden heeft gevraagd voor Security. Mogelijk dat hier kan worden ‘aangehaakt’.
c) Aan het ILT-management voorleggen van de vraag of ILT-personeel dat betrokken is bij Security-controles daarvoor extra gescreend moet worden.
d) Een selectie van exploitanten maken voor de controles.
   - ✓ Voorstel om voor 2020 een 6-tal nog niet op dit onderwerp onderzochte exploitanten te selecteren.
   - ✓ Met name waar de scenario’s diefstal en grote gevaarzetting (toxische stoffen + bovengrondse delen) verwacht wordt.
e) De aanpak uit 2019 voort te zetten:
   - ✓ Inventariserend van karakter.
   - ✓ Rapportages worden ‘encrypted’ opgesteld. Geen papieren exemplaren.
   - ✓ Lege vragenlijst wordt vooraf toezenden.
f) Verdieping (2021?) voorbereiden op zaken zoals op:
   - ✓ Kwaliteit analyse op kwetsbaarheid.
   - ✓ Bepalen meerdere Security-dreiging scenario’s, incl. pad-analyses.
   - ✓ Exploitanten laten oefenen met Security-scenario’s. Met name het preventieve karakter (voorkómen van Security incidenten) is daarbij van belang.

   Mogelijk dat dit samen met Velin kan worden opgepakt (zie ook punt 5b).

Bijlagen (Holmes, Vragenlijst audit, Algemene info Security)

Handreiking invullen Security resultaten Holmes 18dec2019

-> betekent ínvullen'

2016_AIB_HHRB_Buisleidingtoezicht Audit 2017

2016_AIB_HHRB_Audit Algemeen

- De audit is gericht op: **PDCA-cyclus**
- Thema: **Security**
- Op welke elementen (bijlage bij art. 4 Bevb) ligt de nadruk? **3,4,8**
- 2016_AIB_HHRB_Zorgplicht (artikelen 4.1 Bevb) **->**
- 2016_AIB_HHRB_Voorkoming ongewone voorvallen (artikel 4.2 bevb) **->**
- Hoe goed is de kwaliteit van de door de exploitant ingevolge het Revb getroffen technische en organisatorische maatregelen (art. 4.5 Bevb)? **->**
- Komen in dit systeem alle 12 elementen uit de bijlage bij artikel 4 Bevb aan de orde (art. 4.6 Bevb)? **Nee (niet: 1,7,10)**
- 2016_AIB_HHRB_Waardering van de in de audit opgenomen elementen (3,4,8) **->**

Rest is n.v.t.

In map documenten: mogen (in Word) uitnodiging, agenda etc.

Resultaten (rapportage, ingevuld vragenlijsten) mogen alleen encrypted (7zip) documenten.

Fred Huisman

Departementaal vertrouwelijk
Vetgedrukt staan per vraag eventuele opmerkingen en nadere toelichting van de auditor

De vragenlijsten / rapportage <bedrijf>. Securitycontrole d.d. <datum>

-Inventariserende audit[2]-

Versie 2019

Wettelijke basis voor Securitycontroles:

Bevb art. 4 (zorgplicht), art. 10 (ongewone voorvallen); NEN 3655 art. 5.4 (RI&E, bewust uitgevoerde externe verstoringen)

Security managementsystemen: Er zijn diverse managementsystemen die bedrijven moeten 'wapenen' tegen ongewenste beïnvloeding van buitenaf:

- ISPS: International Ship and Port facility Security Code met minimumeisen voor beveiliging van schepen, havenfaciliteiten en overheidsinstellingen. Geldt met name voor locatie waar een wal-schip connectie is (schip ligt aan de kade). Vanuit IMO (international maritime organization) verplicht.
- ISO-NEN-IEC 27001 (2016): internationale standaard voor informatiebeveiliging. Denk aan bescherming van persoons- en bedrijfsgegevens, bescherming tegen hackers, en het weerbaar zijn tegen calamiteiten. (Cyberaanvallen) Op vrijwillige basis.
- ISO-NEN 22301: Business continuity management system (BCMS) ter bescherming tegen, verkleining van de kans op, voorbereiding op, reactie op en herstel van verstorende incidenten wanneer deze zich voordoen. Op vrijwillige basis.

De vragenlijsten: zijn opgesteld aan de hand van de handreiking 'Securitymanagementsysteem' van het Ministerie van IenM . Als maatwerk voor Bevb controles zijn vragen soms geherformuleerd of aangevuld. Ingevulde vragenlijsten krijgen vanwege het vertrouwelijke karakter van de informatie, de ILT-interne rubricering "Departementaal Vertrouwelijk"[3].

Alle antwoorden die worden gegeven moeten ook blijken uit praktijkvoorbeelden, documenten, registraties of rapporten. Deze dienen tijdens de controle beschikbaar zijn voor de onderzoekers van de ILT.

Het gaat bij de controle op het indelen van de performance op de categorieën:

Cat.	Duiding
1	= basisniveau, startend
2	= reeds verder in opbouw
3	=volledig geïmplementeerd

In de vragenlijst wordt + / - 'gescoord' :

Score	Waardering
+	= voldoende
-	= onvoldoende
+ / -	= tussen + en -

Per score wordt door de onderzoeker (waar nodig) kort een tekstuele toelichting gegeven.

Gesproken met: <naam, functie>
Auditor: <naam ILT-inspecteur>

Algemene opmerkingen gesteld vanuit ots:

•

[2] Op basis van interviews. Verificatie door het inzien van stukken heeft slechts beperkt plaatsgevonden en verificatie door het beoordelen van praktijksituaties heeft geheel niet plaatsgevonden.
[3] Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013)

Samenvattende tabel: (zie op volgende pagina's voor onderliggende deellijsten)

Vragenlijst Security weerbaarheid Bevb				
Kerndoelstelling: Het opstellen van een framework waarin Security op een doelmatige, structurele, integrale en efficiënte wijze wordt ingericht. De getroffen fysieke, personele, organisatorische en logische (ICT) maatregelen bieden een adequaat en passend antwoord op in- en externe risico's veroorzaakt door kwaadwillig menselijk handelen. Security benadering begint doorgaans met het vaststellen van het Securitybeleid. Daarna volgt de stap van de risicoanalyse, 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. Het afstemmen met externe (hulp)diensten en/of stakeholders kan een maatregel zijn van de stappen ontwerp, implementatie en beheer van maatregelen.				
Nr.	**Activiteit**	**Categorie**		
		1:Basis niveau	**2: Verder in opbouw**	**3: Volledig**
1	**Security beleidsplan, of –bij een beperkte omvang van het bedrijf- een Security beleidsintentie.** De eisen: Een organisatie formuleert beleid om haar doelstelling te kunnen realiseren. Men heeft een bepaald doel voor ogen. Is door het bedrijf onderkend dat Security inbreuken kunnen plaatsvinden? En is beschreven hoe de organisatie Security op een doelmatige, structurele, integrale en efficiënte wijze zal inrichten ter bescherming tegen kwaadwillig menselijk handelen? **BEVINDINGEN: <NIVEAU: BASIS/OPBOUW/VOLLEDIG>.** Korte toelichting (zie ook de deellijsten): <Korte duiding>			
2	**Risicoanalyse.** De eisen: De risicoanalyse, bij de exploitanten veelal bekend als RI&E, is een weging van de kansen en gevolgen van een ongewenste gebeurtenis. Hij leidt tot inzicht in de impact en waarschijnlijkheid van die gebeurtenis en in de weerbaarheid van een organisatie tegen bedreigingen van vastgestelde belangen, uitval en verstoringen van kritische processen. Die weerbaarheid wordt afgemeten aan de maatregelen die zijn genomen om de waarschijnlijkheid op verstoring te verminderen en de gevolgen beheersbaar te maken. Uiteindelijk komt uit de analyse een risicobeeld dat ertoe kan toe leiden om extra maatregelen te treffen. **BEVINDINGEN:<NIVEAU: BASIS/OPBOUW/VOLLEDIG>.**Korte toelichting (zie ook de deellijsten): <Korte duiding>			
3	**Operator Security Plan.** De eisen: Een operator Security plan of beveiligingsmaatregelenplan geeft aan welke operationele beveiligingsmaatregelen gelden om gedefinieerde bedrijfsbelangen tegen benoemde dreigingen te beschermen. Het betreft beveiligingsmaatregelen van bijvoorbeeld fysieke, personele, organisatorische en logische (ICT) aard. Securitymaatregelen kunnen in routinematige situaties en in bijzondere dreigingsituaties optreden. Daarnaast is vastgelegd op welk wijze deze maatregelen beheerd worden. **BEVINDINGEN: <NIVEAU: BASIS/OPBOUW/VOLLEDIG>.** Korte toelichting (zie ook de deellijsten): <Korte duiding>			

4	**Het afstemmen met externe (hulp-) diensten (of EBO[4]).** De eisen: De interne beveiligingsmaatregelen van een bedrijf zijn afgestemd met de op de beveiliging gerichte maatregelen van externen zoals gemeente, de regiopolitie en eventueel andere partners/stakeholders (bijvoorbeeld externe beveiligingsorganisaties). De afstemming is vastgelegd. **BEVINDINGEN: <NIVEAU: BASIS/OPBOUW/VOLLEDIG>.**Korte toelichting (zie ook de deellijsten): <Korte duiding>			

[4] EBO= Externe beveiligingsorganisatie.

Deellijst Securitybeleid

Security Beleid 2012				
Kerndoelstelling Securitybeleid: Een organisatie formuleert beleid om haar doelstelling te kunnen realiseren. Men heeft een bepaald doel voor ogen. In een Security beleidsplan staat opgenomen hoe de organisatie Security op een doelmatige, structurele, integrale en efficiënte wijze zal inrichten ter bescherming tegen kwaadwillig menselijk handelen. Wanneer een organisatie een beleidsintentieverklaring of gelijkwaardig heeft opgesteld die anders is dan de onderstaande aanpak maar wel in staat is adequaat beleid te voeren is de doelstelling van deze stap ook bereikt.				
Nr.	**Onderdeel**	**Basis niveau**	**Verder in opbouw**	**Volledig**
1	Is er sprake van een separaat op Security gericht managementsysteem voor de Bevb buisleidingen. Denk bijvoorbeeld aan ISPS (beveiliging schip/haven), ISO-NEN 27001 (informatiebeveiliging) of ISO-NEN 22301 (continuïteit bedrijfsvoering)? **<bevinding>**			
2	In het beleid/verklaring zijn de hoofdlijnen van het Securitybeleid opgenomen. Bijvoorbeeld: uitgangspunten, reikwijdte en succesfactoren/indicatoren die de kwaliteit ervan aantonen resp. voor verbetering voordragen. En wanneer/in welke situatie de Securitycyclus wordt herhaald. **<bevinding>**			
3	In het VBS is iemand aangewezen die verantwoordelijk is voor het Securitymanagement. **<bevinding>**			
4	De verantwoordelijkheden en bevoegdheden voor personen in de Securityorganisatie zijn beschreven/opgenomen. Dit kan bijvoorbeeld zijn weergegeven in een organogram. Of functie informatie formulieren. **<bevinding>**			
5	Het opleidingsniveau voor de bij het Securitymanagement betrokken functionarissen is gedefinieerd en de aanwezige kennisniveaus zijn gedocumenteerd. **<bevinding>**			
6	De financiële middelen (budget) voor de Security aanpak zijn in kaart gebracht en afdoende voor een adequate aanpak. *- Waaruit blijkt dat het budget voldoende is?* **<bevinding>**			
7	Er is sprake van effectieve informatieverstrekking omtrent de Securityorganisatie en aanpak. *- Hoe wordt over Security gecommuniceerd tussen de diverse lagen binnen de organisatie?* *- Hoe worden externen (contractors) geïnformeerd?* **<bevinding>**			
8	Er is periodiek/gepland beleidsoverleg waarin de voortgang aangaande Security wordt besproken. *-bijvoorbeeld in de jaarlijkse managementreview* **<bevinding>**			

Deellijst Risicoanalyse/RI&E gericht op Security

Risicoanalyse

Kern doelstelling risicoanalyse:
De risicoanalyse is een weging van de kansen en gevolgen van een ongewenste gebeurtenis. Hij leidt tot inzicht in de impact én waarschijnlijkheid van die gebeurtenis. Dit leidt tot inzicht in de weerbaarheid van een organisatie tegen bedreigingen van vastgestelde belangen en uitval en verstoringen van kritische processen. Die weerbaarheid wordt afgemeten aan de maatregelen die zijn genomen om de kans/waarschijnlijkheid op verstoring te verminderen en de gevolgen beheersbaar te maken. Uiteindelijk komt uit de analyse een risicobeeld die er kan toe leiden dat extra maatregelen moeten worden getroffen.
Wanneer een organisatie een risicoanalyse anders dan de onderstaande aanpak heeft uitgevoerd, en hierdoor in staat is adequate maatregelen te nemen, is de doelstelling van deze stap ook bereikt. Let daarbij wel op het verschil tussen Safety en Security.

Nr.		Onderdeel	Basis niveau	Verder in opbouw	Volledig
1	Voor bereiding	Er is een vastgesteld, duidelijk plan van aanpak voor het opstellen van een Bevb-georiënteerde en op Security gerichte risicoanalyse. Met daarin scope, diepgang en betrokkenheid (in- externen). Mogelijk onderdeel van de RI&E. **<bevinding>**			
2		Er is vastgelegd wanneer een risicoanalyse wordt herzien of opnieuw –eventueel op kleinere schaal- wordt uitgevoerd. Bijvoorbeeld bij veranderingen in het productieproces of tijdens onderhoudswerkzaamheden. **<bevinding>**			
3		Er is een breed team aan vertegenwoordigers van verschillende expertisegebieden betrokken bij het uitvoeren van de Security-risicoanalyse. Denk aan dreiging expertise en technische expertise van het bedrijf zelf. **<bevinding>**			
4		De meest voor de hand liggende Security scenario's (risico's) zijn in kaart gebracht. **<bevinding>**			
5	Afhankelijkheid analyse	De voor het bedrijf belangrijke (Bevb-gerelateerde) bedrijfsonderdelen, processen, objecten en/of gevaarlijke onderdelen zijn geïdentificeerd en in kaart gebracht. Deze belangen worden ook wel "vital assets" genoemd. Vaak beschreven in een systeemoverzicht, plattegrond of organogram. **<bevinding>**			
6		De eventuele gevolgen voor de organisatie bij uitval/verstoring van deze "vital assets" zijn in kaart gebracht. Dit geldt ook voor situaties met externe beïnvloeding, zoals bijvoorbeeld bij sabotage bij een stroomleverancier. **<bevinding>**			
7		De eventuele gevolgen voor de omgeving bij uitval/verstoring van deze "assets" zijn in kaart gebracht geclassificeerd en gedocumenteerd. Dit geldt ook voor ongewenste externe beïnvloeding, zoals sabotage bij een stroomleverancier. **<bevinding>**			
8		De "vital assets" zijn op afhankelijkheid gerangschikt in verschillende niveaus. De uitkomst van de analyse zijn gedocumenteerd, geclassificeerd en passend/afdoende afgeschermd. **<bevinding>**			

9	**Dreiging-analyse**	Specifiek voor Bevb leidingen kan gedacht worden aan scenario's als diefstal, sabotage en terrorisme. De meest relevante dreiging scenario's zijn in kaart gebracht en voorzien van daderprofielen en daden, motivatie en middelen. Denk, naast fysieke dreiging, ook aan 'logische' (ICT) beïnvloeding van besturingssystemen (SCADA[5], Cyber-Security). **<bevinding>**			
10		De uitkomsten van de dreigingsanalyse zijn gedocumenteerd, geclassificeerd en passend/afdoende afgeschermd (bij conflicten met safety-belangen geldt: 'Safety first, Security follows"). **<bevinding>**			
11	**Kwetsbaarheid analyse**	De bestaande maatregelen (fysiek, organisatorisch, personeel, logisch) zijn in kaart gebracht en onderbouwd ten opzichte van de vastgestelde dreigingen via bijvoorbeeld een pad-analyse. **<bevinding>**			
12		Geconstateerde uitkomsten –eventuele kwetsbaarheden- zijn gedocumenteerd en passend/afdoende afgeschermd. **<bevinding>**			
13	**Risico-weging**	De impact van een scenario/risico voor het bedrijf en omgeving is geclassificeerd aan de hand van een vaste systematiek (bijvoorbeeld ingeschatte impact is klein, middel, groot). **<bevinding>**			
14		De waarschijnlijkheid van een scenario/risico is geclassificeerd aan de hand van een vaste systematiek (bijvoorbeeld ingeschatte kans is laag, middel, hoog). **<bevinding>**			

[5] SCADA (Supervisory Control and Data Acquisition) is een besturingssysteem voor industriële processen die bijvoorbeeld in de productie-, energie-, water- en transportsector worden gebruikt.

Deellijst Operator Security Plan

Maatregelenplan (Operator Security Plan)				
Kerndoelstelling maatregelenplan (Operator Security Plan): Een Operator Security Plan of beveiligingsmaatregelenplan geeft aan welke operationele beveiligingsmaatregelen gelden om gedefinieerde bedrijfsbelangen tegen benoemde dreigingen te beschermen. Dit kunnen beveiligingsmaatregelen zijn van bijvoorbeeld fysieke-, personele-, organisatorische en logische aard. De maatregelen kunnen in routinematige situaties en in bijzondere dreigingsituaties zijn/worden getroffen. Daarnaast is vastgelegd op welk wijze deze maatregelen beheerd/onderhouden worden.				
Nr.	**Onderdeel**	**Basis niveau**	**Verder in opbouw**	**Volledig**
1	Er is een actueel overzicht van huidige Securitymaatregelen (maatregelenplan). Gedocumenteerd en passend/afdoende geclassificeerd en afgeschermd **<bevinding>**			
2	Er zijn evenwichtige, efficiënte en samenhangende maatregelenpakketten samengesteld, gekoppeld aan de dreiging scenario's, met een specifiek beveiligingsdoel. **<bevinding>**			
3	De maatregelen worden actueel gehouden en worden vernieuwd/aangepast als daar aanleiding toe is (nieuwe risicoanalyse, nieuwe dreiging scenario's). **<bevinding>**			
4	Er is een kosten-batenanalyse (KBA) uitgevoerd aangaande de ontworpen Securitymaatregelen en deze KBA is gedocumenteerd (de baten zijn lastig uit te drukken; heeft het bedrijf beleid of een norm/oplossing?). **<bevinding>**			
5	Er is een onderhoud- en beheersplan om de getroffen maatregelen op voldoende kwaliteit te houden (gedocumenteerd en met voldoende financiële middelen). **<bevinding>**			

Deellijst afstemming met externe (hulp-) diensten

Afstemming externe (hulp)diensten				
Kerndoelstelling afstemming externe (hulp)diensten Het afstemmingsplan handelt over de afstemming van de interne beveiligingsmaatregelen van een bedrijf met de maatregelen van op de beveiliging gerichte externe hulpdiensten zoals de gemeente, de regiopolitie en eventueel andere diensten.				
Nr.	**Onderdeel**	**Basis niveau**	**Verder in opbouw**	**Volledig**
1	Er is regelmatig (minimaal 2 x per jaar) contact met externe (hulp)diensten op het gebied van beveiliging. Dit kan samen met Safety overleg plaatsvinden, mits Security een duidelijk en op zichzelf staand onderwerp is. **<bevinding>**			
2	Bij de contacten met externe (hulp)diensten op het gebied van beveiliging wordt ook relevantie (dreiging) informatie uitgewisseld. **<bevinding>**			
3	Met de externe (hulp)diensten is afgesproken op welke wijze zij reageren bij de verschillende scenario's. De verwachtingen over-en-weer zijn vastgesteld en gedocumenteerd. **<bevinding>**			
4	Er wordt regelmatig (minimaal 1 x per jaar) geoefend met de externe (hulp)diensten op het gebied van beveiliging. De oefeningen worden geëvalueerd en de resultaten worden gedocumenteerd. Eventuele verbeteringen worden doorgevoerd in de documentatie die afdoende is geclassificeerd en afgeschermd. **<bevinding>**			

Departementaal vertrouwelijk
Vetgedrukt staan per vraag eventuele opmerkingen en nadere toelichting van de auditor

Algemene info Security

Introductie Securitymanagementsysteem (SMS)
Securitymanagement heeft te maken met het borgen van continuïteit van de onderneming (assetmanagement) respectievelijk de vitale infrastructuur van NL. En de beperking van gevaren voor de omgeving, die kunnen ontstaan als gevolg van aanslagen en sabotage (externe veiligheid).

Securitymanagement gaat tenminste over de volgende elementen:

5. Een vastgesteld Securitybeleid.
6. Risico-identificatie en –analyse (risicomanagement).
7. Securitymaatregelen en voorzieningen.
8. Afspraken over de interne en externe Securityorganisatie.

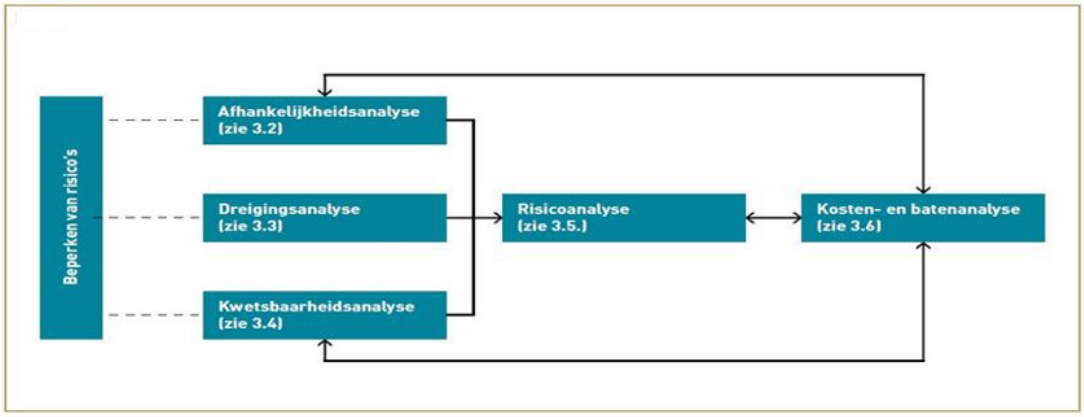
Organisatorische en personele beveiligingsmaatregelen worden samen met bouwkundige en elektronische voorzieningen (waaronder ICT) ingezet om de Security doelstellingen te bereiken. Dat maakt Securitymanagement een complex vak. Het vraagt om een gestructureerde, planmatige en *systematische* aanpak. Door het inrichten en onderhouden van een *Security management*systeem wordt het mogelijk de Security doelstellingen efficiënt en effectief te realiseren.

Risicomanagement
Om een goede risicoanalyse te kunnen uitvoeren is kennis en informatie nodig over het bedrijf, over concrete en potentiële dreigingen én over maatregelen die de weerbaarheid van een bedrijf verhogen. Doel van de risicoanalyse is om in te spelen op ernstige risico's van nu en in de nabije toekomst.
Drie belangrijke aspecten dragen bij aan de risico's die een bedrijf loopt, te weten de onderwerpen:

d) Bedrijfsbelangen.
e) Dreiging.
f) Kwetsbaarheid.

Ad a) De bedrijfsbelangen betreffen de vitale bedrijfsprocessen en cruciale onderdelen van het bedrijf. Deze belangen, waarvan het bedrijf afhankelijk is voor het bereiken van zijn doelstelling, moeten beschermd worden om ernstige bedrijfseconomische of maatschappelijke schade te voorkomen.
Ad b) De dreiging hangt af van de mogelijkheden van potentiële daders (capability) en de mate waarin zij bereid zijn om hun daad uit te voeren (intent). Tijdens de risico-inventarisatie en –analyse zal deze dreiging in kaart moeten worden gebracht. Daarbij is de doelstelling het meten van de bereidheid en de mogelijkheden van de daders en deze vervolgens te rangschikken op de mate van gevaar die zij voor het bedrijf opleveren.
Ad c) De kwetsbaarheid hangt af van de mogelijkheden die de omgeving deze potentiële daders biedt. De weerbaarheid van een bedrijf (getroffen beveiligingsmaatregelen) is in dit kader belangrijk.
Let op: Wanneer men zich echter op risico's oriënteert - dus naast de dreiging, de kwetsbaarheid en het belang in de overwegingen meeneemt - is het niet uitgesloten dat men ondanks een lage dreiging grote risico's moet vaststellen.

Risicoanalyse Security, schematisch



Referenties: Security handreikingen in Security-kaders.nl